IEEE Xplore RELEASE 2.4

Welcome United States Patent and Trademark Office

:::View Selected Items

BROWSE   SEARCH   IEEE XPLORE GUIDE

Results for " (((cascade or cascaded or order or ordered or sequence)and (access or entry) and (security or ✉ e-mail secu... "

Your search matched **12** of **1632036** documents. You selected **12** items.

Display Format: ◯ Citation   ◉ Citation & Abstract

Article Information   View: 1-12 | Viev

» **Download Citations**

[Citation & Abstract ▾]

[ASCII Text ▾] »

» **Learn more**

» **Key**

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

1. **A temporal access control mechanism for database systems**
    Bertino, E.; Bettini, C.; Ferrari, E.; Samarati, P.
    Knowledge and Data Engineering, IEEE Transactions on
    Volume: 8 Issue: 1 Feb 1996
    Page(s): 67-80
    Digital Object Identifier 10.1109/69.485637
    Summary: The paper presents a discretionary access control model in which authoriz
    temporal intervals of validity. An authorization is automatically revoked when the assoc
    interval expires. The proposed model provides rules for the.....
    AbstractPlus | References | Full Text: PDF   **IEEE JNL**

2. **A logic for state transformations in authorization policies**
    Yun Bai; Varadharajan, V.
    Computer Security Foundations Workshop, 1997. Proceedings., 10th
    10-12 Jun 1997
    Page(s): 173-182
    Digital Object Identifier 10.1109/CSFW.1997.596810
    Summary: In a multi-user information-sharing system, an authorization policy provides
    and control access to system, applications and information. In the real world, an autho
    temporal properties. That is, it needs to be .....
    AbstractPlus | Full Text: PDF   **IEEE CNF**

3. **Biometric identification through speaker verification over telephone lines**
    Gonzalez-Rodriguez, J.; Gruz-Llanas, S.; Ortega-Garcia, J.
    Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnal
    on
    1999
    Page(s): 238-242
    Digital Object Identifier 10.1109/CCST.1999.797919
    Summary: In this paper, the identity of a remote user is verified through his voice by n
    telephone in order to gain access to a specific system or service. We have used state-
    independent speaker modeling algorithms, likelihood .....
    AbstractPlus | Full Text: PDF   **IEEE CNF**

4. **A fast automaton-based method for detecting anomalous program behaviors**
    Sekar, R.; Bendre, M.; Dhurjati, D.; Bollineni, P.
    Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on
    2001
    Page(s): 144-155
    Digital Object Identifier 10.1109/SECPRI.2001.924295
    Summary: Anomaly detection on system call sequences has become perhaps the mo
    approach for detecting novel intrusions. A natural way for learning sequences is to use
    automaton (FSA). However previous research indicates that FSA-lea.....
    AbstractPlus | Full Text: PDF   **IEEE CNF**

5. **Performance analysis on new biometric gait motion model**
ChewYean Yam; Nixon, M.S.; Carter, J.N.
Image Analysis and Interpretation, 2002. Proceedings. Fifth IEEE Southwest Symposii
2002
Page(s): 31-34
Digital Object Identifier 10.1109/IAI.2002.999884
Summary: Recognising people by the way they walk and/or run is new. A novel analy
is invariant to human gait of walking and running is developed based on the concept o
coupled oscillators and the biomechanics of human walking and.....

AbstractPlus | Full Text: PDF   IEEE CNF

6. **Design validation of ZCSP with SPIN**
Beaudenon, V.; Encrenaz, E.; Desbarbieux, J.-L.
Application of Concurrency to System Design, 2003. Proceedings. Third International (
18-20 June 2003
Page(s): 102- 110
Digital Object Identifier 10.1109/CSD.2003.1207704
Summary: We consider the problem of specifying a model of the zero copy secured ⌡
purpose of LTL verification with the SPIN model checker. ZCSP is based on direct mei
Data is directly read/written in user space memory, decreasing la.....

AbstractPlus | Full Text: PDF   IEEE CNF

7. **sTuples: semantic tuple spaces**
Khushraj, D.; Lassila, O.; Finin, T.
Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 200
Annual International Conference on
22-26 Aug. 2004
Page(s): 268- 277
Digital Object Identifier 10.1109/MOBIQ.2004.1331733
Summary: Tuple spaces offer a coordination infrastructure for communication betwee
entities by providing a logically shared memory along with data persistence, transactio
well as temporal and spatial decoupling - properties that ma.....

AbstractPlus | Full Text: PDF   IEEE CNF

8. **A first step towards formal verification of security policy properties for RBAC**
Drouineaud, M.; Bortin, M.; Torrini, P.; Sohr, K.
Quality Software, 2004. QSIC 2004. Proceedings. Fourth International Conference on
8-9 Sept. 2004
Page(s): 60- 67
Digital Object Identifier 10.1109/QSIC.2004.1357945
Summary: Considering the current expansion of IT-infrastructure, the security of the ⟨
infrastructure becomes increasingly important. Therefore, assuring certain security pro
systems by formal methods is desirable. So far in secur.....

AbstractPlus | Full Text: PDF   IEEE CNF

9. **Analysis and Modeling of Advanced PIM Architecture Design Tradeoffs**
Upchurch, E.; Sterling, T.; Brockman, J.
Supercomputing, 2004. Proceedings of the ACM/IEEE SC2004 Conference
06-12 Nov. 2004
Page(s): 12- 12
Digital Object Identifier 10.1109/SC.2004.11
Summary: A major trend in high performance computer architecture over the last two
migration of memory in the form of high speed caches onto the microprocessor semicc
Where temporal locality in the computation is high, caches prove.....

AbstractPlus | Full Text: PDF   IEEE CNF

10.
Token based path authorization at interconnection points between hybrid netwo
lambda grid
Gommans, L.; de Laat, C.; Meijer, R.
Broadband Networks, 2005 2nd International Conference on

3-7 Oct. 2005
Page(s): 1378- 1385 Vol. 2
Digital Object Identifier 10.1109/ICBN.2005.1589768

Summary: In order to provide cost effective transport services for highly demanding c
applications, National Research Networks (NRNs) are considering additional types of ɛ
network infrastructures. Next to traditional IP access.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

11. A Scalable and IntrusionÂ¿tolerant Digital TimeÂ¿stamping System
Tulone, D.
Communications, 2006. ICC '06. IEEE International Conference on
Volume: 5 June 2006
Page(s): 2357-2363
Digital Object Identifier 10.1109/ICC.2006.255122

Summary: Secure digital timeÂ¿stamps play a crucial role in many applications that rɛ
correctness of timeÂ¿sensitive information. WellÂ¿known timeÂ¿stamping systems aɼ
linking schemes which provide a relative temporal order by linking reque.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

**12. U biquitous Semantic Space: A context-aware and coordination middleware for ʟ
Computing**
Sudha, R.; Rajagopalan, M.R.; Selvanayaki, M.; Selvi, S.Thamarai
Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd Int
Conference on
7-12 Jan. 2007
Page(s): 1-7
Digital Object Identifier 10.1109/COMSWA.2007.382562

Summary: Ubiquitous Computing poses the challenge of increased communication, cɪ
and functionality. In a highly dynamic and weekly connected ubiquitous environment, ɕ
to the network (synchronous communication) is very difficult......

AbstractPlus | Full Text: PDF   **IEEE CNF**

View: **1-12** | **View Search Resɪ**

Help   Contact Us   Privacy & ɪ

IEEE *Xplore*

Welcome United States Patent and Trademark Office

View Selected Items   **BROWSE   SEARCH   IEEE XPLORE GUIDE**

Results for " (((sequence or order or ordered or cascade or cascaded) and (access or entry) and (secure or   ✉e-mail
securit... "
Your search matched **733** of **1632036** documents. You selected **25** items.

Display Format: ○ Citation   ◉ Citation & Abstract

Article Information   View: 1-25 | Vie\

» **Download Citations**

| Citation & Abstract ▼ |

| ASCII Text ▼ | ≫

» Learn more

» **Key**

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

1. **An n-grid model for group authorization**
   Wen-Gong Shieh; Weems, B.; Kavi, K.M.
   Computer Security Applications Conference, 1990., Proceedings of the Sixth Annual
   3-7 Dec 1990
   Page(s): 384-392
   Digital Object Identifier 10.1109/CSAC.1990.143813
   Summary: The n-grid model for group authorization and access control extends the N representation of two-dimensional partial orders and incorporates the implicit authoriza model. The n-grid is a representation of multi-dimensional partial .....
   AbstractPlus | Full Text: PDF   **IEEE CNF**

2. **A temporal access control mechanism for database systems**
   Bertino, E.; Bettini, C.; Ferrari, E.; Samarati, P.
   Knowledge and Data Engineering, IEEE Transactions on
   Volume: 8 Issue: 1 Feb 1996
   Page(s): 67-80
   Digital Object Identifier 10.1109/69.485637
   Summary: The paper presents a discretionary access control model in which authoriz temporal intervals of validity. An authorization is automatically revoked when the assoc interval expires. The proposed model provides rules for the.....
   AbstractPlus | References | Full Text: PDF   **IEEE JNL**

3. **Reducing manpower intensive tasks through automation of security technologie**
   Carback, R.T.
   Security Technology, 1995. Proceedings. Institute of Electrical and Electronics Engine
   1995 International Carnahan Conference on
   18-20 Oct 1995
   Page(s): 331-339
   Digital Object Identifier 10.1109/CCST.1995.524932
   Summary: Security in today's government and commercial environments is changing. to provide manpower against security threats is diminishing. Risk management is prefe avoidance. In order for management to ensure that the appropriat.....
   AbstractPlus | Full Text: PDF   **IEEE CNF**

   Multiple intelligent agent supported Internet security system: issues, current sol proposed approach
   Lin Zeng; huaiqing Wamg; Lee, M.K.O.
   Intelligent Processing Systems, 1997. ICIPS '97. 1997 IEEE International Conference
   Volume: 1 28-31 Oct 1997
   Page(s): 920-922 vol.1
   Digital Object Identifier 10.1109/ICIPS.1997.672965
   Summary: The Internet has become a common target to attack because of security cc of incidents, such as attempted and successful intrusions, have grown dramatically. Se have shown that many individuals and companies are abstaining .....
   AbstractPlus | Full Text: PDF   **IEEE CNF**

[Handwritten note:]
Search string:
(cascade or cascaded or sequence or order or ordered) and
(access or entry) and
(security or secure or authorize or authorization)

5. **Specifying application-level security in workflow systems**
Olivier, M.S.; van de Riet, R.P.; Gudes, E.
Database and Expert Systems Applications, 1998. Proceedings. Ninth International W
25-28 Aug 1998
Page(s): 346-351
Digital Object Identifier 10.1109/DEXA.1998.707423
Summary: A workflow process involves the execution of a set of related activities over a specific task. Security requires that such activities may only be performed by authori order to enforce such requirements, access to the u.....

AbstractPlus | Full Text: PDF IEEE CNF

6. **A contextual role-based access control authorization model for electronic patien**
Motta, G.H.M.B.; Furuie, S.S.
Information Technology in Biomedicine, IEEE Transactions on
Volume: 7 Issue: 3 Sept. 2003
Page(s): 202- 207
Digital Object Identifier 10.1109/TITB.2003.816562
Summary: The design of proper models for authorization and access control for elect record (EPR) is essential to a wide scale use of EPR in large health organizations. In t propose a contextual role-based access control authorizatio.....

AbstractPlus | References | Full Text: PDF IEEE JNL

7. **Human computer interaction through consolidation and visualization for order e**
Toyoda, S.; Niki, N.; Nishitani, H.
Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual In
Conference of the IEEE
Volume: 2 17-21 Sept. 2003
Page(s): 1280- 1283 Vol.2
Digital Object Identifier 10.1109/IEMBS.2003.1279500
Summary: In this paper, we propose a human computer interaction model through cc visualization for order entry systems. This model makes effective use of the patient da features 1) the consolidation of order data, 2) the visualizatio.....

AbstractPlus | Full Text: PDF IEEE CNF

8. **Secure access to corporate resources in a multi-access perspective: needs, pro solutions**
Casole, M.; Yi Cheng
Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 4:
22-25 April 2003
Page(s): 482- 489
Summary: The modern businessman needs to access corporate resources constantl the access location, thus improving effectiveness. In order to accomplish this, a numbe technologies allow mobile users to be connected to some kind of n.....

AbstractPlus | Full Text: PDF IEE CNF

9. **A first step towards formal verification of security policy properties for RBAC**
Drouineaud, M.; Bortin, M.; Torrini, P.; Sohr, K.
Quality Software, 2004. QSIC 2004. Proceedings. Fourth International Conference on
8-9 Sept. 2004
Page(s): 60- 67
Digital Object Identifier 10.1109/QSIC.2004.1357945
Summary: Considering the current expansion of IT-infrastructure, the security of the c infrastructure becomes increasingly important. Therefore, assuring certain security pro systems by formal methods is desirable. So far in secur.....

AbstractPlus | Full Text: PDF IEEE CNF

10. **Database security - concepts, approaches, and challenges**
Bertino, E.; Sandhu, R.
Dependable and Secure Computing, IEEE Transactions on
Volume: 2 Issue: 1 Jan.-March 2005

Page(s): 2- 19
Digital Object Identifier 10.1109/TDSC.2005.9
Summary: As organizations increase their reliance on, possibly distributed, informatic
daily business, they become more vulnerable to security breaches even as they gain p
efficiency advantages. Though a number of techniques, such.....

AbstractPlus | Full Text: PDF   **IEEE JNL**

11. **Security service adaptation for embedded service systems in changing environr**
Il lner, S.; Pohl, A.; Krumm, H.
Industrial Informatics, 2004. INDIN '04. 2004 2nd IEEE International Conference on
24-26 June 2004
Page(s): 457- 462
Digital Object Identifier 10.1109/INDIN.2004.1417387
Summary: Distributed embedded applications increasingly operate in changing envir
the application security depends on the type and properties of the currently used comr
services and employed devices. While vulnerabilities, threats, and .....

AbstractPlus | Full Text: PDF   **IEEE CNF**

12. **R andom-access control mechanisms using adaptive traffic load in ALOHA and (
for EDGE**
Rivero-Angeles, M.E.; Lara-Rodriguez, D.; Cruz-Perez, F.A.
Vehicular Technology, IEEE Transactions on
Volume: 54 Issue: 3 May 2005
Page(s): 1160- 1186
Digital Object Identifier 10.1109/TVT.2005.844657
Summary: In this paper, three random access control mechanisms based on the well
ALOHA, NP-CSMA, and 1P-CSMA protocols are presented. The basic idea is to limit t
transmissions and retransmissions at high traffic loads in order to m.....

AbstractPlus | References | Full Text: PDF   **IEEE JNL**

13. **N ew authentication method for mobile centric communications**
Hongyuan Chen; Sivakumar, T.V.L.N.
Vehicular Technology Conference. 2005. VTC 2005-Spring. 2005 IEEE 61st
Volume: 5 30 May-1 June 2005
Page(s): 2780- 2784 Vol. 5
Digital Object Identifier 10.1109/VETECS.2005.1543853
Summary: This paper proposes a new authentication scheme for accessing contents
applications in both mobile device and Internet. A user first divide all the contents, sen
applications in both mobile device and the Internet into four gr.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

14. **Job -centric security model for open collaborative environment**
Demchenko, Y.; de Laat, C.; Gommans, L.; Oudenaarde, B.; Tokmakoff, A.; Snijders, I
Collaborative Technologies and Systems, 2005. Proceedings of the 2005 International
15-20 May 2005
Page(s): 69- 77
Digital Object Identifier 10.1109/ISCST.2005.1553296
Summary: This paper describes the design and development of a flexible, customer (
infrastructure for open collaborative environments. The experiences were gained withii
of the collaboratory.nl project. The work is based on exten.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

15.
**Expl olting Hierarchical Identity-Based Encryption for Access Control to Pervasi\
Information**
Hengartner, U.; Steenkiste, P.
Security and Privacy for Emerging Areas in Communications Networks, 2005. Secure(
International Conference on
05-09 Sept. 2005
Page(s): 384- 396
Digital Object Identifier 10.1109/SECURECOMM.2005.18

Summary: Access control to confidential information in pervasive computing environr challenging for multiple reasons: First, a client requesting access might not know whicl are necessary in order to be granted access to the requested inf.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

16. **A Multi-dimension Rule Update In a TCAM-based High-Performance Network Se**
Hae-Jin Jeong; Il-Seop Song; Taeck-Geun Kwon; Yoo-Kyoung Lee
Advanced Information Networking and Applications, 2006. AINA 2006. 20th Internatior
Volume: 2 18-20 April 2006
Page(s): 62- 66
Digital Object Identifier 10.1109/AINA.2006.37
Summary: Network security systems such as firewall and intrusion prevention systerr packet classification rule to allow or protect the network traffic. In addition, they are for multi-gigabit speed in order to deploy the current Inter.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

17. **Fr ameworks for Secured Business Process Management Systems**
Haeng-Kon Kim; Roger Y. Lee; Hae-Sool Yang
Software Engineering Research, Management and Applications, 2006. Fourth Internat
on
09-11 Aug. 2006
Page(s): 57- 65
Digital Object Identifier 10.1109/SERA.2006.38
Summary: This paper formally defines a role-driven security and access control modi process in order eventually to provide a theoretical basis for realizing the secured busi management systems. That is, we propose a graphical repre.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

18. **Design of security state machine of access control for control object based on II**
Bin Duan; Bing Liu
Power Engineering Society General Meeting, 2006. IEEE
18-22 June 2006
Page(s): 3 pp.-
Digital Object Identifier 10.1109/PES.2006.1709328
Summary: Access control with identity authentication becomes crucial for critical circi operation in the substation automation system. According to IEC 61850, the implemen control policy depends on a virtual access view. But the sta.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

19. **Security Constraints in Access Control of Information System Using UML Langu**
Ane ta Poniszewska-Maranda
Enabling Technologies: Infrastructure for Collaborative Enterprises, 2006. WETICE '0€
International Workshops on
June 2006
Page(s): 332-337
Digital Object Identifier 10.1109/WETICE.2006.58
Summary: Process of security administration in an information system is a complex ta constraints should be expressed in order to define in the proper way the security policy constraints can be classified into two groups. The fir.....

AbstractPlus | Full Text: PDF   **IEEE CNF**

20. **Qu antifiable Security Metrics for Large Scale Heterogeneous Systems**
Syed Naqvi; Michel Riguidel
Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE Inti
Oct. 2006
Page(s): 209-215
Digital Object Identifier 10.1109/CCST.2006.313452
Summary: The exponential growth of information technology and the prospect of incre access to the computing, communications, and storage resources have made these s) vulnerable to attacks. Use of heterogeneous devices and communication li.....

21. Secu rity for FTTx Optical Access Networks

Walid Shawbaki; Ahmed Kamal
Local Computer Networks, Proceedings 2006 31st IEEE Conference on
Nov. 2006
Page(s): 221-228
Digital Object Identifier 10.1109/LCN.2006.322103
Summary: Passive optical networks (PONs) is the answer to increasing demand on b;
enabler for Fiber To The x (FTTx) implementation, where x can be Home (FTTH), Curl
Building (FTTB). However, PONs use shared fiber link with broadcast a.....

22. Chaotic functions for generating binary sequences and their suitability in Multip

M andi, Mahalinga V.; Murali, R.; Haribhat, K.N.
Communication Technology, 2006. ICCT '06. International Conference on
Nov. 2006
Page(s): 1-4
Digital Object Identifier 10.1109/ICCT.2006.341812
Summary: Chaotic sequences have good correlation properties and they can be used
sequences in Spread Spectrum Communication. Chaotic functions are highly sensitive
condition and exhibit non-linear behavior. In Chaotic spread spectrum com.....

23. C oncurrency Control using Subject- and Purpose-Oriented (SPO) View

Enokido, Tomoya; Takizawa, Makoto
Availability, Reliability and Security, 2007. ARES 2007. The Second International Conf
10-13 April 2007
Page(s): 454-464
Digital Object Identifier 10.1109/ARES.2007.60
Summary: In information systems, multiple transactions issued by subjects manipulat
conflicting way. Conflicting access requests from multiple transactions have to be seri
various ways to order multiple access requests like FIFO.....

24. C ontext-Aware Access Control Making Access Control Decisions Based on Con

Lachmund, Sven; Walter, Thomas; Gomez, Laurent; Bussard, Laurent; Olk, Eddy
Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conferer
17-21 July 2006
Page(s): 1-8
Digital Object Identifier 10.1109/MOBIQW.2006.361782
Summary: In ubiquitous computing environments access control decisions have to be
changes of the situation or state of an entity, in order to properly adjust to these chang
need of manual interaction. A solution to this challenge is.....

25. R ole-based Concurrency Control in a Subject- and Purpose-Oriented (SPO) View

Enokido, Tomoya; Barolli, Valbona; Takizawa, Makoto
Advanced Information Networking and Applications, 2007. AINA '07. 21st International
21-23 May 2007
Page(s): 171-178
Digital Object Identifier 10.1109/AINA.2007.124
Summary: In information systems, processes have to be scheduled to share a limited
resource objects like memory and CPU with other processes. In database systems, co
requests from multiple transactions have to be serialized. There ar.....

PORTAL
USPTO

THE ACM DIGITAL LIBRARY   ☞ Feedb:

✱ Search String same as for IEEE Search ✱

Terms used:
sequence or **order** or **ordered** or **cascade** or **cascaded** and **access** or **entry** and **secure** or **security** or **authoriz**

Sort results by [relevance ▾]   ◈ Save results to a Binder
Display results [expanded form ▾]   ⚃ Search Tips
                                                  ☐ Open results in a new window

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next
Best 200 shown

1   A taxonomy for secure object-oriented databases
Martin S. Olivier, Sebastiaan H. von Solms
March 1994   **ACM Transactions on Database Systems (TODS)**, Volume 19 Issue 1
Publisher: ACM Press
Full text available: 📄 pdf(3.05 MB)   Additional Information: full citation, abstract, referen

> This paper proposes a taxonomy for secure object-oriented databases in order to clarify the issu
> indicates some implications of the various choices one may make when designing such a databa
> relational databases. The object-oriented database model is more complex than the relational n
> databases are more complex than ...

> **Keywords**: formal security models, information security, multilevel secure databases, object-o

2   The relational model for database management: version 2
E. F. Codd
January 1990   Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: 📄 pdf(28.61 MB)   Additional Information: full citation, abstract, referen

> **From the Preface (See Front Matter for full Preface)**

> An important adjunct to precision is a sound theoretical foundation. The relational model is soli
> logic and the theory of relations. This book, however, does not dwell on the theoretical foundati
> that I now perceive as important for database users, and therefore for DBMS vendors. My perce

3   A model of OASIS role-based access control and its support for active security
Jean Bacon, Ken Moody, Walt Yao
November 2002   **ACM Transactions on Information and System Security (TISSEC)**, Volume 5
Publisher: ACM Press
Full text available: 📄 pdf(352.06 KB)   Additional Information: full citation, abstract, referen

> OASIS is a role-based access control architecture for achieving secure interoperation of service:
> to allow autonomous management domains to specify their own access control policies and to in
> Services define roles and implement formally specified policy to control role activation and serv
> appropriate context, in order to activat ...

Keywords: Certificates, OASIS, RBAC, distributed systems, policy, role-based access control, s

4 Propagation of authorizations in distributed database systems
Pierangela Samarati, Paul Ammann, Sushil Jajodia
November 1994   **Proceedings of the 2nd ACM Conference on Computer and communicatio**
Publisher: ACM Press
Full text available: pdf(1.40 MB)   Additional Information: full citation, abstract, referen

We consider the propagation of authorizations in distributed database systems. If no constraint
then the authorization states at different sites may evolve inconsistently. A standard solution is
appear as if they had occurred in some serial order at a single site, perhaps via an atomic comr
result in authorization changes ...

5 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982   Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB)   Additional Information: full citation, abstract, referen

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prol
have come to rely on these systems to process and store data, we have also come to wonder a

Data security is the science and study of methods of protecting data in computer and communi

6 A rule-based framework for role-based delegation and revocation
Longhua Zhang, Gail-Joon Ahn, Bei-Tseng Chu
August 2003   **ACM Transactions on Information and System Security (TISSEC)**, Volume 6
Publisher: ACM Press
Full text available: pdf(1.05 MB)   Additional Information: full citation, abstract, referen

Delegation is the process whereby an active entity in a distributed environment authorizes anot
systems, a user often needs to act on another user's behalf with some subset of his/her rights.
requirements with ad-hoc mechanisms by compromising existing disorganized policies or simpl
there is a strong need in the large, distrib ...

Keywords: Role, access control, delegation, revocation, rule-based

7 Access control with IBM Tivoli access manager
Günter Karjoth
May 2003   **ACM Transactions on Information and System Security (TISSEC)**, Volume 6
Publisher: ACM Press
Full text available: pdf(367.07 KB)   Additional Information: full citation, abstract, referen

Web presence has become a key consideration for the majority of companies and other organiz
the Web is increasingly being regarded as an extension of the organization itself, directly integr
takes place, security grows in importance. IBM Tivoli Access Manager offers a shared infrastruc
technologies that have begun to emerge in the com ...

Keywords: Access control, WWW security, Web servers, authorization management

8 Fast detection of communication patterns in distributed executions

Thomas Kunz, Michiel F. H. Seuren

November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies (**

Publisher: IBM Press

Full text available: pdf(4.21 MB)   Additional Information: full citation, abstract, referen

Understanding distributed applications is a tedious and difficult task. Visualizations based on pr understanding of the execution of the application. The visualization tool we use is Poet, an ever these diagrams are often very complex and do not provide the user with the desired overview c repeated occurrences of n on-trivial commun ...

9 Access control: On the modeling and analysis of obligations

Keith Irwin, Ting Yu, William H. Winsborough

October 2006 **Proceedings of the 13th ACM conference on Computer and communicatio**

Publisher: ACM Press

Full text available: pdf(230.18 KB)   Additional Information: full citation, abstract, referen

Traditional security policies largely focus on access control requirements, which specify who car control requirements, the availability of services in many applications often further imposes obl taken by a subject in the future as a condition of getting certain privileges at present. However policies are concerning the security ...

Keywords: obligations, policy

10 Macintosh human interface guidelines

Apple Computer, Inc.

January 1992 Book

Publisher: Addison-Wesley Publishing Company

Full text available: pdf(37.61 MB)   Additional Information: full citation, abstract, referen

Macintosh Human Interface Guidelines describes the way to create products that optimize the ii explains the whys and hows of the Macintosh interface in general terms and specific details.

Macintosh Human Interface Guidelines helps you link the philosophy behind the Macintosh inter Examples from a wide range of Macintosh products show good human interface design, includin

11 Limitations of the Kerberos authentication system

S. M. Bellovin, M. Merritt

October 1990 **ACM SIGCOMM Computer Communication Review**, Volume 20 Issue 5

Publisher: ACM Press

Full text available: pdf(1.12 MB)   Additional Information: full citation, abstract, citings,

The Kerberos authentication system, a part of MIT's Project Athena, has been adopted by other number of limitations and some weaknesses. Some are due to specifics of the MIT environment discuss a number of such problems, and present solutions to some of them. We also demonstre needed in some cases.

12 A calculus for access control in distributed systems

Martín Abadi, Michael Burrows, Butler Lampson, Gordon Plotkin

September 1993 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, v

Publisher: ACM Press

Full text available: pdf(1.94 MB)   Additional Information: full citation, abstract, referen

We study some of the concepts, protocols, and algorithms for access control in distributed syst principal may come to believe that another principal is making a request, either on his own or c

for accesss control lists and theories for deciding whether requests should be granted.

Keywords: cryptographic protocols, cryptography, modal logic

13 Approaches to fault-tolerant and transactional mobile agent execution---an algorithmic viev

Stefan Pleisch, André Schiper

September 2004   **ACM Computing Surveys (CSUR)**, Volume 36 Issue 3

Publisher: ACM Press

Full text available: pdf(946.94 KB)   Additional Information: full citation, abstract, referen

Over the past years, mobile agent technology has attracted considerable attention, and a signif
develop mobile agent technology, reliability mechanisms such as fault tolerance and transactior
field of fault-tolerant and transactional mobile agent execution and thus at guiding the reader t
existing approaches. It starts with a discu ...

Keywords: ACID, Byzantine failures, agreement problem, asynchronous system, commit, cras
replication, security, transaction

14 Query evaluation techniques for large databases

Goetz Graefe

June 1993   **ACM Computing Surveys (CSUR)**, Volume 25 Issue 2

Publisher: ACM Press

Full text available: pdf(9.37 MB)   Additional Information: full citation, abstract, referen

Database management systems will continue to manage large data volumes. Thus, efficient alg
sequences will be required to provide acceptable performance. The advent of object-oriented ar
On the contrary, modern data models exacerbate the problem: In order to manipulate large set
systems manipulate simple records, query-processi ...

Keywords: complex query evaluation plans, dynamic query evaluation plans, extensible datab
operator model of parallelization, parallel algorithms, relational database systems, set-matchin(

15 Secure operating systems: Towards a VMM-based usage control framework for OS kernel

Min Xu, Xuxian Jiang, Ravi Sandhu, Xinwen Zhang

June 2007   **Proceedings of the 12th ACM symposium on Access control models and t**

Publisher: ACM Press

Full text available: pdf(485.61 KB)   Additional Information: full citation, abstract, referen

Protecting kernel integrity is one of the fundamental security objectives in building a trustworth
approaches and systems have been proposed and developed. However, access control models t
capture important security requirements such as continuous policy enforcement and mutable pi
protection mechanisms in these systems reside in the ...

Keywords: UCON, VMM, access control, authorization, kernel integrity, operating system prote

16 UIO: a uniform I/O system interface for distributed systems

David R. Cheriton

January 1987   **ACM Transactions on Computer Systems (TOCS)**, Volume 5 Issue 1

Publisher: ACM Press

Full text available: pdf(3.20 MB)   Additional Information: full citation, abstract, referen

A uniform I/O interface allows programs to be written relatively independently of specific I/O se

available in a distributed environment. Ideally, the interface provides this uniform access withoi
performance. However, a uniform interface does not arise from careful design of individual syst
paper, the UIO (unifo ...

17 Peer-to-peer infrastructure: Pastiche: making backup cheap and easy
Landon P. Cox, Christopher D. Murray, Brian D. Noble
December 2002   **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI
Publisher: ACM Press
Full text available: pdf(1.65 MB)   Additional Information: full citation, abstract, referen

Backup is cumbersome and expensive. Individual users almost never back up their data, and bi
presents *Pastiche*, a simple and inexpensive backup system. Pastiche exploits excess disk capa
costs. Each node minimizes storage overhead by selecting peers that share a significant amoun
peers, and peers with high ove ...

18 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructi
Albert Levi, M. Ufuk Caglayan, Cetin K. Koc
February 2004   **ACM Transactions on Information and System Security (TISSEC)**, Volume 7
Publisher: ACM Press
Full text available: pdf(532.64 KB)   Additional Information: full citation, abstract, referen

Certification is a common mechanism for authentic public key distribution. In order to obtain a
network of certificates, which is called public key infrastructure (PKI), and verify the certificate:
Nested certification is a novel methodology for efficient certificate path verification. Basic idea i:
other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

19 Distributed operating systems
Andrew S. Tanenbaum, Robbert Van Renesse
December 1985   **ACM Computing Surveys (CSUR)**, Volume 17 Issue 4
Publisher: ACM Press
Full text available: pdf(5.49 MB)   Additional Information: full citation, abstract, referen

Distributed operating systems have many aspects in common with centralized ones, but they al
introduction to distributed operating systems, and especially to current university research aboi
operating system and how it is distinguished from a computer network, various key design issu
projects are examined in some detail ...

20 Access management for distributed systems: Role-based cascaded delegation
Roberto Tamassia, Danfeng Yao, William H. Winsborough
June 2004   **Proceedings of the ninth ACM symposium on Access control models and t**
Publisher: ACM Press
Full text available: pdf(218.61 KB)   Additional Information: full citation, abstract, referen

We propose *role-based cascaded delegation*, a model for delegation of authority in decentralize
cascaded delegation combines the advantages of role-based trust management with those of ca:
implementation of role-based cascaded delegation using Hierarchical Certificate-Based Encrypti
long role-based delegation chain is captur ...

Keywords: RBAC, access control, delegation, trust management

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9

```
Set     Items    Description
S1      327854   (COMPUTER?(2N)SYSTEM? ? OR NETWORK? OR DISTRIBUT? OR ETHER-
                 NET? OR INTERNET OR INTRANET? OR LAN OR LANS OR WAN OR WANS OR
                 WLAN? ? OR VLAN? ?)(7N)(CONTROL? OR REGULAT? OR DIRECT? OR M-
                 ANAG? OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR
                 SUPERVIS???)
S2      248932   (PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD? OR ENF-
                 ORC?)(3N)(ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI? OR
                 USING)
S3      195926   (ORDER?()SET? ? OR SEQUEN? OR PATTERN? OR ORDER?)(5N)(LEVE-
                 L? OR STEP? ? OR STAGE? OR TIER?? ? OR OPERATION? OR FUNCTION?
                 OR COMMAND?)
S4       26666   S3(5N)(TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO-
                 N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR
                 MINUTE? ? OR SECOND? ? OR PERIOD?)
S5       33021   S3:S4(5N)(SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE
                 OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADD-
                 ITIONAL)
S6        8606   S4:S5(5N)(PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? -
                 OR OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?)()OUT
                 OR COMPLET? OR ENABL? OR ALLOW?)
S7          25   S6 AND S2 AND S1
File 350:Derwent WPIX 1963-2007/UD=200752
         (c) 2007 The Thomson Corporation
File 347:JAPIO Dec 1976-2007/Mar(Updated 070809)
         (c) 2007 JPO & JAPIO
```

7/69,K/2   **(Item 2 from file: 350)**
(DIALOG(R) File 350:Derwent WPIX)
(c) 2007 The Thomson Corporation. All rts. reserv.

0015035617 - Drawing available
WPI ACC NO: 2005-383609/200539
XRPX Acc No: N2005-310943
Trail/path protection function enhancement method in synchronous optical network, involves mapping content of bytes of section overhead into path overhead bytes at low/high order level, for handling protective resources
Patent Assignee: ALCATEL (COGE)
Inventor: CAZZANIGA G; SESTITO V
Patent Family (3 patents, 33 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20050099941	A1	20050512	US 2004822667	A	20040413	200539	B
EP 1531566	A1	20050518	EP 2003292866	A	20031112	200539	E
CN 1617476	A	20050518	CN 200410042594	A	20040525	200558	E

Priority Applications (no., kind, date): EP 2003292866 A 20031112

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20050099941	A1	EN	16	7	
EP 1531566	A1	EN			

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI
   FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Alerting Abstract US A1
   NOVELTY - The content of bytes of section overhead are mapped in a linear multiplex section protection (MSP) N:1 trail protection function by protocol exchange, into path overhead (POH) bytes at low order and/or high order level, so as to allow handling of multiple protective resources shared among different working resources in both end-to-end handling and intermediate handling.
   DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

   1.network element;

   2.trail/path protection function enhancement program; and

   3.computer readable medium storing trail/path protection function enhancement program.

   USE - For enhancing trail/path **protection** function in **synchronous** optical network (SONET) and synchronous digital hierarchy (SDH) network.
   ADVANTAGE - Enhances the features of standardized protection scheme. Eliminates requirement of operating system application to the operator, thereby improving traffic **management** reliability in **network** .
   DESCRIPTION OF DRAWINGS - The figure shows the schematic diagram of the network elements.
   NEa,NEb network elements

Title Terms/Index Terms/Additional Words: TRAILING; PATH; PROTECT; FUNCTION
   ; ENHANCE; METHOD; SYNCHRONOUS; OPTICAL; NETWORK; MAP; CONTENT; BYTE;
   SECTION; OVERHEAD; LOW; HIGH; ORDER; LEVEL; HANDLE; RESOURCE

Class Codes
International Classification (Main): G01R-031/08
International Classification (+ Attributes)

```
IPC + Level Value Position Status Version
  H04J-0003/14  A  I     R  20060101
  H04Q-0011/04  A  N     R  20060101
  H04J-0003/14  C  I     R  20060101
  H04Q-0011/04  C  N     R  20060101
US Classification, Issued: 370907000, 370228000
```

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-F02C2; T01-N02B2C; T01-S03; W01-A06A1;
  W01-A06C1; W01-A06E
   Alerting Abstract ...USE – For enhancing trail/path **protection** function
in **synchronous** optical network (SONET) and synchronous digital hierarchy
(SDH) network...

...standardized protection scheme. Eliminates requirement of operating
system application to the operator, thereby improving traffic **management**
reliability in **network** .

Original Publication Data by Authority

Original Abstracts:
...protocol exchange into POH bytes of the path overhead in SDH or SONET,
at Low **Order** and/or High **Order** **level** , so as **to** **allow** the
handling of **more** than **one** protecting **resource** shared **among**
different working resources, both in end-to-end handling and in
intermediate handling...

...in SDH or SONET, at Low Order and/or High Order level, so as to **allow**
the **handling** of **more** than **one** protecting resource shared among
different working resources, both in **end** - **to** -end **handling** and **in**
intermediate **handling.** >
Claims:
...protocol exchange into POH bytes of the path overhead in SDH or SONET,
at Low **Order** and/or High **Order** **level** , so as **to** **allow** the
handling of **more** than **one** protecting **resource** shared **among**
different working resources, both in end-to-end handling and in
intermediate handling...

...protocol exchange into POH bytes of the path overhead in SDH or SONET,
at Low **Order** and/or High **Order** **level** , so as to **allow** the **handling**
of more than one protecting resource shared among **different** working
resources, both **in** end-to-end **handling** **and** in intermediate **handling.**
>

0014416207 - Drawing available
WPI ACC NO: 2004-606295/200459
Related WPI Acc No: 2004-634023; 2004-634025
XRPX Acc No: N2004-479628
Coprocessor e.g. graphics processing unit, task scheduling method, involves processing tasks by coprocessor in order indicated by run list, where coprocessor switches to next task in event of occurrence of any switching event
Patent Assignee: GOSSALIA A B (GOSS-I); MICROSOFT CORP (MICT); PRONOVOST
  S (PRON-I)
Inventor: GOSALIA A B; GOSSALIA A B; LANGLEY B; LANGLEY B L; NAGASE H;
  PRONOVOST S
Patent Family (9 patents, 35 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
EP 1450258	A2	20040825	EP 20043544	A	20040217	200459	B
JP 2004252983	A	20040909	JP 200442173	A	20040218	200459	E
US 20040187122	A1	20040923	US 2003448399	P	20030218	200463	E
			US 2003448400	P	20030218		
			US 2003448402	P	20030218		
			US 2003474513	P	20030529		
			US 2004763778	A	20040122		
US 20040187135	A1	20040923	US 2003448399	P	20030218	200463	E
			US 2003448400	P	20030218		
			US 2003448402	P	20030218		
			US 2004777797	A	20040212		
US 20040231000	A1	20041118	US 2003448400	P	20030218	200477	E
			US 2004779272	A	20040213		
US 20050168472	A1	20050804	US 2003448399	P	20030218	200552	E
			US 2003748362	A	20031230		
			US 200589856	A	20050325		
CN 1609812	A	20050427	CN 200410039767	A	20040213	200558	E
IN 200400206	I1	20060331	IN 2004DE206	A	20040213	200625	NCE
IN 200400207	I1	20060303	IN 2004DE207	A	20040213	200639	E

Priority Applications (no., kind, date): US 200589856 A 20050325; US
  2004779272 A 20040213; IN 2004DE206 A 20040213; US 2004777797 A
  20040212; US 2003748362 A 20031230; US 2003474513 P 20030529; US
  2003448399 P 20030218; US 2003448400 P 20030218; US 2003448402 P
  20030218; US 2004763778 A 20040122

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 1450258	A2	EN	64	26	

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI
  FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Number	Kind	Lan	Pg	Dwg	Filing Notes	
JP 2004252983	A	JA	145			
US 20040187122	A1	EN			Related to Provisional	US 2003448399
					Related to Provisional	US 2003448400
					Related to Provisional	US 2003448402
					Related to Provisional	US 2003474513
US 20040187135	A1	EN			Related to Provisional	US 2003448399
					Related to Provisional	US 2003448400
					Related to Provisional	US 2003448402
US 20040231000	A1	EN			Related to Provisional	US 2003448400
US 20050168472	A1	EN			Related to Provisional	US 2003448399
					Continuation of application	US

2003748362
IN 200400206   I1 EN
IN 200400207   I1 EN

Alerting Abstract EP A2
NOVELTY - The method involves generating a run list by a CPU, where the
list comprises a list of tasks to be processed by a coprocessor. The run
list is delivered to a scheduler process that prepares the tasks on the run
list. The tasks are processed by the coprocessor in an order indicated by
the run list. The coprocessor switches to a next task on the run list, when
a switching event e.g. page fault, occurs while processing a task.
DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

  1. a computer readable medium comprising computer executable instructions
     for carrying out a method for scheduling task for processing in a
     coprocessor

  2. a modulated data signal carrying computer executable instructions for
     use in performing a method for scheduling task for processing in a
     coprocessor

  3. a graphics processing unit for performing a method of scheduling tasks
     for processing in a coprocessor.

USE - Used in a computer system for scheduling tasks that are processed
in a coprocessor e.g. a graphics processing unit that performs
three-dimensional graphics calculation to support application e.g. games
and computer aided design.
ADVANTAGE - The method provides the run list and allows the coprocessor
to switch immediately from one task to the next, on the occurrence of a
switching event, without waiting for CPU intervention, thus providing the
CPU with more processing time for other functions and enhancing coprocessor
efficiency and power.
DESCRIPTION OF DRAWINGS - The drawing shows a scheduling model.

Title Terms/Index Terms/Additional Words: GRAPHIC; PROCESS; UNIT; TASK;
  SCHEDULE; METHOD; ORDER; INDICATE; RUN; LIST; SWITCH; EVENT; OCCUR

Class Codes
International Classification (Main): G06F, G06F-009/38, G09G-005/14
 (Additional/Secondary): G06T-001/20, G09G-005/393, G06F-009/46
International Classification (+ Attributes)
IPC + Level Value Position Status Version
  G06F-0009/46 A I   R 20060101
  G06F-0009/48 A I   R 20060101
  G06F-0009/50 A I   R 20060101
  H04N-0007/16 A I   R 20060101
  H04N-0007/173 A I   R 20060101
  G06F-0009/46 C I   R 20060101
  H04N-0007/16 C I   R 20060101
  H04N-0007/173 C I   R 20060101
US Classification, Issued: 718100000, 718104000, 725132000, 725133000,
  725140000, 725141000, 725152000, 345543000

File Segment: EngPI; EPI;
DWPI Class: T01; P85
Manual Codes (EPI/S-X): T01-C04D; T01-M02B; T01-S03

Original Publication Data by Authority

Original Abstracts:

...any one or more of (1) executing rendering commands sent to the coprocessor in a **different** **order** **than** they were **submitted** by **applications** ; (**2**) preempting the coprocessor during **scheduling** **of** non-interruptible hardware; (3) **allowing** user mode drivers to build work items using command buffers in a way that **does** not compromise **security** ; (4) preparing DMA **buffers** for execution while the coprocessor is busy executing a previously prepared DMA buffer; (5) resuming...

...in a computer environment having a main processing unit for executing an operating system and **an** **application** , a **system** memory, and **a** graphics processing unit having an aperture that maps, in a tiled manner, between a portion...

7/69,K/6   (Item 6 from file: 350)

0013999657 - Drawing available
WPI ACC NO: 2004-180864/200417
XRPX Acc No: N2004-143794
**Device for copy-protected distribution of electronic documents via public
electronic data network e.g. the internet, with time-limited access to
reconstruction server for reconstruction of encrypted document**
Patent Assignee: BRAINSHIELD TECHNOLOGIES INC (BRAI-N)
Inventor: WITTKOETTER E; WITTKOTTER E
Patent Family (4 patents, 100 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2004015952	A2	20040219	WO 2003EP8606	A	20030804	200417	B
DE 10335943	A1	20040603	DE 10335943	A	20030804	200436	E
AU 2003266962	A1	20040225	AU 2003266962	A	20030804	200456	E
US 20040181688	A1	20040916	US 2003635798	A	20030805	200461	E

Priority Applications (no., kind, date): DE 10236061 A 20020806

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2004015952	A2	DE	32	2	

National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY
   BZ CA CH CN CO CR CU CZ DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL
   IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO
   NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC
   VN YU ZA ZM ZW
Regional Designated States,Original: AT BE BG CH CY CZ DE DK EA EE ES FI
   FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ
   TR TZ UG ZM ZW

AU 2003266962	A1	EN		Based on OPI patent	WO 2004015952

   Alerting Abstract WO A2
   NOVELTY - The device has a number of subscriber terminals (10), each
assigned to a user, configured for loading access of an electronic document
via the electronic data network, a number of loading accesses carried out
for associated electronic file sections, at least one loading access
effected from a different subscriber terminal assigned to a different user,
with electronic operational sequence instruction data provided by an
instruction data server unit (24) required for performing the loading
accesses. The received file sections are encrypted according to the
operational sequence instruction data to prevent use of the electronic
document before reconstruction via a reconstruction server unit (30),
coupled for a limited time access to a decryption unit (16,18) within the
subscriber terminal.
   DESCRIPTION - An INDEPENDENT CLAIM for a method for copy-protected
distribution of electronic documents via a public electronic data network
is also included.
   USE - The device is **used** for copy- **protected** distribution of
electronic documents to subscriber terminals connected to a public
electronic data network, e.g. the internet.
   ADVANTAGE - Device protects distributed electronic documents from being
read by unauthorized network users.
   DESCRIPTION OF DRAWINGS - The figure shows a schematic block circuit
diagram of a device for copy-protected distribution of electronic documents
via electronic data network. (Drawing includes non-English language text).
   10 Subscriber terminals
   14 Publication unit

16,18 Decryption unit
24 Instruction data server unit
30 Reconstruction server unit

Title Terms/Index Terms/Additional Words: DEVICE; COPY; PROTECT; DISTRIBUTE
; ELECTRONIC; DOCUMENT; PUBLIC; DATA; NETWORK; TIME; LIMIT; ACCESS;
RECONSTRUCT; SERVE; ENCRYPTION
Class Codes
International Classification (Main): H04L-012/22, H04L-029/06, H04L-009/00
(Additional/Secondary): H04L-009/32
US Classification, Issued: 713201000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-N01D2; T01-N02B1

Alerting Abstract ...USE – The device is **used** for copy- **protected**
distribution of electronic documents to subscriber terminals connected to a
public electronic data network, e...

Original Publication Data by Authority

Original Abstracts:
...of electronic documents of a predetermined document data structure in a
publicly accessible electronic data **network**, particularly **the** Internet.
Said device comprises: a number of subscriber terminal units (10), which
are at least...

...to carry out the number of loading accesses, the subscriber terminal
units obtain electronic operational **sequence** instruction **data**, **which**
are **created** **in** a document-specific and/or subscriber-specific manner,
from an instruction data unit (24), particularly...and configured for
combining the encrypted form with a reconstruction file in order to
generate **the** electronic document **for** display by the display unit in an
unencrypted form that can be used by the....
Claims:
...and that represent an encrypted form of said electronic document, at
least one of said **downloads** **being** **from** said second computer and at
least one of said downloads being from said third computer...

DIALOG(R)File-350:Derwent_WPIX

0013865161 – Drawing available
WPI ACC NO: 2004-043742/200404
Related WPI Acc No: 2005-423933; 2006-510379
XRPX Acc No: N2004-035314
Hardware processor for Internet **protocol based storage** network
appliance, provides remote direct **memory access capability on IP and**
Ethernet network **, using transmission** control **protocol, STCP and UDP**
protocol
Patent Assignee: PANDYA A (PAND-I); PANDYA A A (PAND-I)
Inventor: PANDYA A; PANDYA A A
Patent Family (13 patents, 99 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2003104943	A2	20031218	WO 2003US18386	A	20030610	200404	B
US 20040010545	A1	20040115	US 2002388407	P	20020611	200406	E
			US 2003458855	A	20030610		
US 20040010612	A1	20040115	US 2002388407	P	20020611	200406	E
			US 2003459674	A	20030610		
US 20040030757	A1	20040212	US 2002388407	P	20020611	200412	E
			US 2003459297	A	20030610		
US 20040030770	A1	20040212	US 2002388407	P	20020611	200412	E
			US 2003459350	A	20030610		
US 20040030806	A1	20040212	US 2002388407	P	20020611	200412	E
			US 2003459019	A	20030610		
US 20040037299	A1	20040226	US 2002388407	P	20020611	200416	E
			US 2003458844	A	20030610		
US 20040037319	A1	20040226	US 2002388407	P	20020611	200416	E
			US 2003459349	A	20030610		
AU 2003251492	A1	20031222	AU 2003251492	A	20030610	200445	E
US 20040165588	A1	20040826	US 2002388407	P	20020611	200457	E
			US 2003458844	A	20030610		
			US 2003458855	A	20030610		
			US 2003459019	A	20030610		
			US 2003459297	A	20030610		
			US 2003459349	A	20030610		
			US 2003459350	A	20030610		
			US 2003459674	A	20030610		
			WO 2003US18386	A	20030610		
			US 2004783890	A	20040220		
US 20040210320	A1	20041021	US 2002388407	P	20020611	200470	E
			US 2003458844	A	20030610		
			US 2003458855	A	20030610		
			US 2003459019	A	20030610		
			US 2003459297	A	20030610		
			US 2003459349	A	20030610		
			US 2003459350	A	20030610		
			US 2003459674	A	20030610		
			WO 2003US18386	A	20030610		
			US 2004783890	A	20040220		
			US 2004845345	A	20040512		
EP 1573454	A2	20050914	EP 2003757485	A	20030610	200560	E
			WO 2003US18386	A	20030610		
JP 2006516054	W	20060615	WO 2003US18386	A	20030610	200639	E
			JP 2004511951	A	20030610		

Priority Applications (no., kind, date): US 2004845345 A 20040512; US
2004783890 A 20040220; US 2003459674 A 20030610; US 2003459350 A

20030610; US 2003459349 A 20030610; US 2003459297 A 20030610; US
2003459019 A 20030610; US 2003458855 A 20030610; US 2003458844 A
20030610; WO 2003US18386 A 20030610; US 2002388407 P 20020611

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2003104943	A2	EN	232	52	

National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY
BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID
IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ
NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TR TT TZ UA UG UZ VN YU
ZA ZM ZW

Regional Designated States,Original: AT BE BG CH CY CZ DE DK EA EE ES FI
FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ
TR TZ UG ZM ZW

Number	Kind	Lan	Filing Notes	
US 20040010545	A1	EN	Related to Provisional	US 2002388407
US 20040010612	A1	EN	Related to Provisional	US 2002388407
US 20040030757	A1	EN	Related to Provisional	US 2002388407
US 20040030770	A1	EN	Related to Provisional	US 2002388407
US 20040030806	A1	EN	Related to Provisional	US 2002388407
US 20040037299	A1	EN	Related to Provisional	US 2002388407
US 20040037319	A1	EN	Related to Provisional	US 2002388407
AU 2003251492	A1	EN	Based on OPI patent	WO 2003104943
US 20040165588	A1	EN	Related to Provisional	US 2002388407
			C-I-P of application	US 2003458844
			C-I-P of application	US 2003458855
			C-I-P of application	US 2003459019
			C-I-P of application	US 2003459297
			C-I-P of application	US 2003459349
			C-I-P of application	US 2003459350
			C-I-P of application	US 2003459674
			C-I-P of application	WO 2003US18386
US 20040210320	A1	EN	Related to Provisional	US 2002388407
			C-I-P of application	US 2003458844
			C-I-P of application	US 2003458855
			C-I-P of application	US 2003459019
			C-I-P of application	US 2003459297
			C-I-P of application	US 2003459349
			C-I-P of application	US 2003459350
			C-I-P of application	US 2003459674
			C-I-P of application	WO 2003US18386
			C-I-P of application	US 2004783890
EP 1573454	A2	EN	PCT Application	WO 2003US18386
			Based on OPI patent	WO 2003104943

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI
FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Number	Kind	Lan	Pg	Filing Notes	
JP 2006516054	W	JA	64	PCT Application	WO 2003US18386
				Based on OPI patent	WO 2003104943

Alerting Abstract WO A2
NOVELTY - The hardware processor provides remote **direct** memory access
capability on **Internet** protocol (IP) **network** and **Ethernet   network**
using transmission **control** protocol (TCP), STCP and UDP protocol.
DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

1.switching system;

2.network appliance;

3.chip set;

4. hardware implemented ISCSI/IP storage controller ;

5. host processor;

6. host;

7. multi-port hardware processor;

8. integrated circuit hardware processor;

9. remote direct memory access operating method;

10. iSCSI stack;

11. TCP/IP stack;

12. IP processor;

13. multiprocessor system;

14. TCP/IP processor engine;

15. IP storage processor engine;

16. TCP/IP processor;

17. hardware implemented IP network application processor;

18. transport level RDMA function execution method;

19. peer system;

20. cluster of server;

21. CPU;

22. packet scheduler and sequencer;

23. classification resource;

24. Internet protocol packet scheduling and sequencing method;

25. hardware data processing classifier engine;

26. hardware classifier engine method;

27. storage flow and RDMA controller ;

28. commands scheduling and sequencing method;

29. RDMA method;

30. data processing apparatus;

31. session index;

32. session cache and memory complex;

33. session memory;

34. transport layer RDMA protocol execution method;

35.server;

36.hardware processor manufacturing method;

37.IP storage area network switching system line card;

38.gate controller ;

39.storage area network management appliance; and

40. network .

USE - Hardware processor for Internet protocol (IP) based storage network
appliance (claimed) and switching system (claimed). Also used **in**
network management , bandwidth **management** , **firewall and** security
applications.
ADVANTAGE - Reduces TCP/IP protocol stack overhead sharply and enables
high line rate storage and data transport solution based on IP. Provides
features to **terminate TCP** traffic **carrying** the storage and data
payload. Thereby eliminates the TCP/IP networking stack overhead. Allows
packets to pass through from input to output with minimal latency. Enables
high line rate storage or data traffic carried over IP. .
DESCRIPTION OF DRAWINGS - The figure shows a block diagram of the IP
network application processor.

Title Terms/Index Terms/Additional Words: HARDWARE; PROCESSOR; PROTOCOL;
BASED; STORAGE; NETWORK; APPLIANCE; REMOTE; DIRECT; MEMORY; ACCESS;
CAPABLE; IP; TRANSMISSION; CONTROL

Class Codes
International Classification (+ Attributes)
IPC + Level Value Position Status Version
   G05B-0015/00 A I   R 20060101
   G06F-0013/10 A I   F B 20060101
   G06F-0015/173 A I   R 20060101
   G06F-0015/177 A I   R 20060101
   H04L-0012/56 A I   R 20060101
   H04L-0029/06 A I   R 20060101
   H04L-0029/08 A I   R 20060101
   G05B-0015/00 C I   R 20060101
   G06F-0015/16 C I   R 20060101
   H04L-0012/56 C I   R 20060101
   H04L-0029/06 C I   R 20060101
   H04L-0029/08 C I   R 20060101
US Classification, Issued: 709203000, 709230000, 709213000, 709217000,
   709223000, 709220000, 709250000, 709212000, 370401000, 370395500,
   370469000, 370395520, 370389000, 700001000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-F05E; T01-H01B1A; T01-N02A1; T01-N02A3C;
   W01-A03B; W01-A06E1; W01-A06G2; W01-A06G5E

Hardware processor for Internet **protocol based storage** network
appliance, provides remote direct **memory access capability on IP and**
Ethernet network **, using transmission** control **protocol, STCP and UDP**
protocol

   Alerting Abstract ...NOVELTY - The hardware processor provides remote

direct memory access capability on **Internet** protocol (IP) **network** and
Ethernet **network** using transmission **control** protocol (TCP), STCP and
UDP protocol....switching system; network appliance; chip set; **hardware**
implemented ISCSI/IP storage **controller** ; host processor; host; multi-port
hardware processor; integrated circuit hardware processor; remote direct
memory access...

...classification resource; Internet protocol packet scheduling and
sequencing method; hardware data processing classifier engine; hardware
classifier engine method; storage flow and **RDMA** **controller** ; **commands**
scheduling and **sequencing** method; RDMA method; data processing
apparatus; session index; session cache and memory complex; session memory;
transport layer RDMA protocol execution method; server; hardware processor
manufacturing method; IP storage area **network** switching system line card;
gate **controller** ; storage area **network** **management** appliance; and
network .
    ...

...USE – Hardware processor for Internet protocol (IP) based storage
network **appliance** (claimed) and switching system (claimed). Also used **in**
network **management** , bandwidth **management** , **firewall** **and** security
applications.
    ...

...enables high line rate storage and data transport solution based on IP.
Provides features to **terminate** **TCP** traffic **carrying** the storage and
data payload. Thereby eliminates the TCP/IP networking stack overhead.
Allows packets

Original Publication Data by Authority

Original Abstracts:
...Une architecture fournit des possibilites de transport et de traitement
de paquets de Protocole **Internet** (**IP**) depuis la couche 2 par la
terminaison totale TCP/IP et l'inspection complete de...
Claims:
...comprising a hardware processor providing remote direct memory access
capability for enabling data transfer using **TCP** over IP **networks** , said
processor being programmable and sending and receiving data packets' also
having identification information based...

...What is claimed is:1. A hardware processor providing remote
direct memory access capability on an IP **network** and using a TCP, SCTP
or UDP protocol, or a combination of **any** of the foregoing, over IP
networks .

    ...

...packets;b. a session memory for storing IP session information;c. at
least one memory **controller** for **controlling** memory accesses;d. at least
one media interface for coupling to at least one network...a peer, memory
regions reserved for RDMA;l. recording said memory regions reserved for
RDMA **in** an RDMA database and **maintaining** said database;m. executing
operations provided by RDMA capability;n. executing security management
functions;o...

...I claim:1. A **security** system comprising a **network** ,said
network comprising one or more networked systems of one or more types,a
plurality...

...said hardware processor comprisinga protocol processing engine to do transport layer protocol processing; or **a** programmable rule processing engine to analyze **network** traffic for rule matching or **taking** actions on matched rules or a combination thereof; ora security processing engine to do encryption, decryption, authorization or authentication or a combination thereof **using** standard or proprietary **security** protocols; ora packet classification engine to classify the network traffic; ora packet processing

0013706078 - Drawing available
WPI ACC NO: 2003-803229/200375
XRPX Acc No: N2003-643888
**Computer-based maintenance resource system in industrial facility, has
operation interface which receives operation data for scheduling and
assigning resources to execute job plan**
Patent Assignee: FRISINA F (FRIS-I)
Inventor: FRISINA F
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20030187865	A1	20031002	US 2002368022	P	20020327	200375	B
			US 2002147344	A	20020515		

Priority Applications (no., kind, date): US 2002368022 P 20020327; US
  2002147344 A 20020515

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20030187865	A1	EN	42	28	Related to Provisional US 2002368022

   Alerting Abstract US A1
   NOVELTY - The system executes a job planning software for producing job
plan or work orders, based on the information supplied by a user. An
operation interface receives operation data related to generated job plan
or work order, for scheduling and assigning resources to execute job plan
or protection request.
   DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

   1.job plan preparation method;

   2.computer generated work order approved method.

   USE - For maintaining resources in industrial or commercial facility
using computer.
   ADVANTAGE - The operation input and requirement are fully integrated with
maintenance resource allocation and planning requirements by using
operation interface, hence work orders are issued only after achieving
necessary approvals and operation input.
   DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the
computer-based maintenance resource system.
   1 computer
   4 standard database
   5 work order database
   6 integration software component
   8 operation requirement database

Title Terms/Index Terms/Additional Words: COMPUTER; BASED; MAINTAIN;
   RESOURCE; SYSTEM; INDUSTRIAL; FACILITY; OPERATE; INTERFACE; RECEIVE; DATA
   ; SCHEDULE; ASSIGN; EXECUTE; JOB; PLAN

Class Codes
International Classification (Main): G06F-007/00
US Classification, Issued: 707102000

File Segment: EPI;
DWPI Class: T01

Manual Codes (EPI/S-X): T01-J05A2B; T01-J05B4P; T01-N01A2

Original Publication Data by Authority

Original Abstracts:
A computer based maintenance resource **management** **system** has an
operations software component with access to historical operations
requirements such that job plans for the current...
Claims:
...program, and means for integrating the operations data into the job plan
and/or work **order** for use in **scheduling** **and** assigning resources to
execute the job plan and/or **protection** **request.>**

DIALOG(R)File 350:Derwent WPIX

0013565781 - Drawing available
WPI ACC NO: 2003-660043/200362
Related WPI Acc No: 2003-660044; 2007-024009
XRPX Acc No: N2003-526333·
Data network management **and service provider using command line
interface framework, transmits command sequences to corresponding** managed
data network **entity, for execution of command line interface actions in
entity**
Patent Assignee: ALCATEL CANADA INC (COGE); CHAN D W (CHAN-I); KATZ F
  (KATZ-I); LANDRY K E D (LAND-I); MURRAY C (MURR-I); NGO C N (NGOC-I);
  ZABIHI A (ZABI-I)
Inventor: CHAN D W; KATZ F; LANDRY K E D; MURRAY C; MURRAY C W; NGO C N;
  ZABIHI A
Patent Family (7 patents, 32 countries)·

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20030115304	A1	20030619	US 2002115900	A	20020405	200362	B
CA 2365436	A1	20030619	CA 2365436	A	20011219	200362	E
EP 1322066	A2	20030625	EP 2002293097	A	20021213	200362	E
US 7113989	B2	20060926	US 2002115900	A	20020405	200663	E
EP 1322066	B1	20061220	EP 2002293097	A	20021213	200702	E
DE 60216885	E	20070201	DE 60216885	A	20021213	200722	E
			EP 2002293097	A	20021213		
DE 60216885	T2	20070705	DE 60216885	A	20021213	200744	E
			EP 2002293097	A	20021213		

Priority Applications (no., kind, date): CA 2365436   A 20011219; US
  2002115900 A 20020405

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20030115304	A1	EN	13	7	
CA 2365436	A1	EN			
EP 1322066	A2	EN			

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI
  FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

| EP 1322066 | B1 | EN | | | |

Regional Designated States,Original: DE ES FR GB IT

DE 60216885	E	DE			Application EP 2002293097
					Based on OPI patent EP 1322066
DE 60216885	T2	DE			Application EP 2002293097
					Based on OPI patent EP 1322066

  Alerting Abstract US A1
  NOVELTY - A command line interface (CLI) processor (520) processes the
CLI dictionary entries holding vocabulary and grammar specifications of
commands used in interacting with at least one **managed** data **network**
entity (510), on receiving request for CLI actions to be performed from a
managed object server (MOS) (200). A communication module (540) transmits
each CLI command sequence to corresponding network entity, for execution.
  DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

  1.method of interacting with managed data network entity; and

  2.method of providing dictionary of CLI commands.

  USE - For **managing** data **networks** such as wireless local area **network**

(LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers (RAS), distribution nodes providing demultiplexing function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management** , statistics gathering, performance reporting, fault **management** , **network surveillance, service provisioning, billing and accounting and security enforcement using** command line interface framework.

ADVANTAGE - Provides automatic entry of CLI command in dictionary and support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network** entity **management costs and time and improves development and maintenance of the network management** and service provisioning solution.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the data **network management** and service provisioning command line interface framework.

200 managed object server
510 **managed** data **network** entity
520 CLI processor
540 communication module

Title Terms/Index Terms/Additional Words: DATA; NETWORK; MANAGEMENT; SERVICE; COMMAND; LINE; INTERFACE; FRAMEWORK; TRANSMIT; SEQUENCE; CORRESPOND; ENTITY; EXECUTE; ACTION

Class Codes
International Classification (+ Attributes)

IPC +	Level	Value	Position	Status	Version
G06F-0015/173	A	I	F	B	20060101
H04L-0012/24	A	I		R	20060101
H04L-0012/24	A	I	F	B	20060101
H04L-0012/24	A	I	F		20060101
G06F-0015/16	C	I	F	B	20060101
H04L-0012/24	C	I		R	20060101
H04L-0012/24	C	I	F	B	20060101
H04L-0012/24	C	I			20060101
H04L-0012/24	C	I		B	20060101

US Classification, Issued: 709223000, 709222000, 709224000, 709220000, 709223000, 370241000, 370254000, 707100000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-F05B; T01-N02A2; W01-A06B5A; W01-A06E

Data network management **and service provider using command line interface fr**amework, transmits command sequences to corresponding managed **data** network **entity, for execution of command line interface actions in entity**

Alerting Abstract ...entries holding vocabulary and grammar specifications of commands used in interacting with at least one **managed** data **network** entity (510), on receiving request for CLI actions to be performed from a managed object...
...method of interacting with **managed** data **network** entity; and method of providing dictionary of CLI commands...

...USE - For **managing** data **networks** such as wireless local area **network** (LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers...

...function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management ,** statistics gathering, performance reporting, fault **management , network** surveillance, service provisioning, billing and accounting and **security enforcement using** command line interface framework...

...support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network** entity **management** costs and time and improves development and maintenance of the **network management** and service provisioning solution...

...DESCRIPTION OF DRAWINGS – The figure shows the block diagram of the data **network management** and service provisioning command line interface framework...
...510 **managed** data **network** entity...

Original Publication Data by Authority

Original Abstracts:
 A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved form a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved form a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...
...commands in the CLI command sequence are sent for execution. The

solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved form a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is... ...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **net**work **management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution.
Claims:
Network management and service provisioning Command Line Interface (CLI) framework, comprising: a. a processor responsive to...

...holding vocabulary and grammar specifications of a plurality of commands used in interacting with at **least** one **managed** data network entity; and c. a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries wherein** a network management and service provisioning solution is provided making abstraction of the **at** least **one** managed data network entity...

...A Command Line Interface (CLI) **framework for** a network **manager** (NM) that manages **a** plurality of managed entities **of** a communication network, comprising: a CLI dictionary (530) holding vocabulary and grammar specifications for all...

...sequence of commands required to configure a managed entity that said managed object represents in **response** to **said event** and handling **execution** of **said** sequence of commands at said managed entity; anda communications module (540) for transmitting said sequence of commands to

said managed entity for execution, and interpreting results **received** from said managed **entity** , **wherein** a network management and service provisioning solution is provided making abstraction of the type of...

...I/we **claim** : 1 . A network management and service provisioning Command Line Interface (CLI) framework, comprising: a. a processor...

...entries holding vocabulary and grammar specifications of a plurality of commands used in interacting with **at** least **one** managed data network entity; and c. a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries** **wherein** a network management and service provisioning solution is provided making abstraction of the **at** least **one** managed data network entity...

...We claim:1. A Command Line Interface (CLI) framework **component** **of** a Network Management System (**NMS**), the NMS managing a plurality **of** field **installed** managed communications network entities **of** a communications network, **each** field **installed** managed communications network entity being represented and modeled by an associated managed object instance stored...

...database associated with the NMS, the CLI framework component comprising: a. a CLI dictionary codifying **a** plurality **of** managed communications network entity-specific **CLI** commands and maintaining at least one **mapping** between **the** managed communications network entity-specific CLI commands **and** a corresponding managed object type;b. a generic processor executing coded logic to: i. detect...

...responsive to the detected event selectively generate a sequence of CLI commands required to configure **the** field **installed** managed communications network entity **associated** with said managed object instance by consulting the CLI dictionary;iii. handle execution of said sequence of CLI commands at **said** field **installed** managed communications network entity, including interpreting CLI command execution results received from **said** field **installed** managed communications network entity; andiv. generating an error report based on an unsuccessful execution...

...the execution results; andc.`a communications module transmitting said sequence of CLI commands to **said** field **installed** managed communications network entity to be executed thereon, and conveying the execution results received from **said** field **installed** managed communications network entity to the generic **processor** , **wherein** a network management and service provisioning solution is provide **making** abstraction **of** managed communications network entity types.

‹DIALOG(R) File 350:Derwent WPIX›
(c) 2007 The Thomson Corporation. All rts. reserv.

0008061777 - Drawing available
WPI ACC NO: 1997-157344/199715
XRPX Acc No: N1997-129878
Access control **method for resources in** distributed **systems - involves obtaining object references that include unforgable numbers and supplying these references to server objects**
Patent Assignee: SUN MICROSYSTEMS INC   (SUNM)
Inventor: NESSETT D M; TOCK T D
Patent Family (8 patents, 8 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
EP 762289	A2	19970312	EP 1996306020	A	19960816	199715	B
JP 9251425	A	19970922	JP 1996234642	A	19960819	199748	E
TW 314609	A	19970901	TW 1996112101	A	19961003	199803	E
KR 1997012183	A	19970329	KR 199634970	A	19960819	199815	E
US 5742759	A	19980421	US 1995516671	A	19950818	199823	E
CN 1149797	A	19970514	CN 1996113317	A	19960817	200123	E
EP 762289	B1	20040721	EP 1996306020	A	19960816	200449	E
DE 69632938	E	20040826	DE 69632938	A	19960816	200456	E
			EP 1996306020	A	19960816		

Priority Applications (no., kind, date): EP 1996306020 A 19960816; US
   1995516671 A 19950818

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 762289	A2	EN	13	3	
Regional Designated States,Original: DE FR GB IT					
JP 9251425	A	JA	14		
TW 314609	A	ZH			
US 5742759	A	EN	14		
EP 762289	B1	EN			
Regional Designated States,Original: DE FR GB IT					
DE 69632938	E	DE			Application EP 1996306020
					Based on OPI patent EP 762289

Alerting Abstract EP A2
  The access control method involves a user operating at a display device
(107) and establishes a authenticated link to the computer (101). The
computer or the system has a client object (117) and a number of server
objects (119,121). When the user logs on the client object obtains details
of the associated membership group (123).
  The client object can communicate with the server objects to identify
objects that will be required. The server objects return a reference that
includes an unforgable number. When the user makes a print request, it
passes the object reference. The print server uses these to obtain approved
access to other servers.
  ADVANTAGE - Provides simple and efficient "delegation" handling of user
access rights.

Title Terms/Index Terms/Additional Words: ACCESS; CONTROL; METHOD; RESOURCE
  ; DISTRIBUTE; SYSTEM; OBTAIN; OBJECT; REFERENCE; NUMBER; SUPPLY; SERVE

Class Codes
International Classification (Main): G06F-001/00, G06F-012/00, G06F-012/14,
  G06F-015/00, H04L-009/00
  (Additional/Secondary): G06F-013/00, G06F-017/21, G06F-009/46, G09C-001/00

Access control **method for resources in** distributed **systems...**

Original Titles:
...Method and system for **securely** **controlling** **access** to system
resources in a **distributed** system...

...Method and system for **securely** **controlling** **access** to system
resources in a **distributed** system...

...METHOD AND SYSTEM FOR **CONTROLLING** **SECURITY** OF **ACCESS** TO SYSTEM
RESOURCE IN **DISTRIBUTED** SYSTEM...

...Method and system for facilitating access **control** to system resources
in a **distributed** **computer** **system** .

Original Publication Data by Authority

Original Abstracts:
Embodiments of the present invention provide an improve method and system
for **securely** **controlling** access to **resources** **in** **a** **distributed**
computer ^**system** . One **embodiment** **of** **the** present invention stores
and binds a group identification to a target object and then uses...
...Embodiments of the present invention provide an improved method and
system for **securely** **controlling** **access** to resources in a **distributed**
  computer **system** . One **embodiment** **of** **the** present invention stores
and **binds** **a** **group** identification to a target object and then uses
membership checking to determine whether a client...

...the present invention avoids performing costly cryptographic operations
in order to verify access rights of **requesting** objects, as **was** common
in some prior art systems. A **second** embodiment of the present invention
stores and binds a group identification to a target object...
Claims:
1. A method executed in a **computer** **system** **for** **controlling** access
to system resources **in** a **distributed** **computer** **system** , **the**
method comprising the steps of: sending a request from a client object to
a spreadsheet server...

...A method executed in a **computer** **system** (101) for **controlling**
access to system resources in a **distributed** **computer** **system**
comprising:</br>   sending a request (201) from a client object (117) to a
spreadsheet server object to bind a group identifier to a spreadsheet
object;</br>   under **control** of the spreadsheet server object;</br>
obtaining **a** **spreadsheet** object (205);</br>   **storing** the group
identifier with the spreadsheet **object** (**207**);</br>   **generating** an
unforgeable checksum (209);</br>   storing the unforgeable checksum with
the spreadsheet object (209);</br>   sending the...A method executed in
a **computer** **system** for facilitating access **control** to system resource
in a **distributed** **computer** **system** , the **distributed** **computer**
system including a first server object, a target object, a client object
and a second server...

...of the objects belonging to one or more specified groups of objects residing in the **computer** **system** , the method comprising the steps of:under **control** of the first server object,storing a group identifier associated with the target object in...

...group of object in the computer system with access privileges to the target object;under **control** of the second server object,sending **an access** request to the **first** server object requesting access to **the target** **object** , the **access** **request** **including** a second server principal identifier which identifies a principal operating the second server object;under...

...target object, the target object reference indicating a location of the target object in the **computer** **system** ;under **control** of the client object,locating a second server object which operates on behalf of a

DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0008978289 - Drawing available
WPI ACC NO: 1998-532222/199845
Related WPI Acc No: 1998-532211; 1998-532223; 1998-532433; 1999-024004;
  2002-470358
XRPX Acc No: N1998-415231
**Dynamic client registry for distribution of information over network - in
which information from client entities on different networks is organized
for selective sharing**
Patent Assignee: BURNS T A (BURN-I); BUTMAN R A (BUTM-I); DOUGHERTY J C
  (DOUG-I); KMIEC M D (KMIE-I); MALONE T J (MALO-I); PFN INC (PFNP-N);
  RAMACHANDRAN R (RAMA-I)
Inventor: BURNS T A; BUTMAN R A; DOUGHERTY J C; KMIEC M D; MALONE T J;
  RAMACHANDRAN R
Patent Family (5 patents, 80 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 1998043184	A1	19981001	WO 1998US5731	A	19980324	199845	B
AU 199867701	A	19981020	AU 199867701	A	19980324	199909	E
US 6026430	A	20000215	US 1997828833	A	19970324	200016	E
EP 1019850	A1	20000719	EP 1998913067	A	19980324	200036	E
			WO 1998US5731	A	19980324		
JP 2002515156	W	20020521	JP 1998545903	A	19980324	200236	E
			WO 1998US5731	A	19980324		

Priority Applications (no., kind, date): US 1997828833 A 19970324

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 1998043184	A1	EN	132	47	

National Designated States,Original: AL AM AT AU AZ BA BB BG BR BY CA CH
  CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC
  LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL
  TJ TM TR TT UA UG US UZ VN YU ZW
Regional Designated States,Original: AT BE CH DE DK EA ES FI FR GB GH GM
  GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 199867701	A	EN			Based on OPI patent WO 1998043184
EP 1019850	A1	EN			PCT Application WO 1998US5731
					Based on OPI patent WO 1998043184

Regional Designated States,Original: AT BE CH DE DK ES FI FR GB GR IE IT
  LI LU MC NL PT SE

JP 2002515156	W	JA	128		PCT Application WO 1998US5731
					Based on OPI patent WO 1998043184

  Alerting Abstract WO A1
  The registry is used to organise information from client entities on
different networks for selective sharing, and includes a computer for
storing a dynamic client registry and resource locators containing function
names.
  A web server causes the computer to respond to the resource locators by
loading the function name indicated. A database management program
organises the dynamic client registry.
  USE - Providing **control** over **distribution** , redistribution, **access
security** , filtering, organizing and display of information across
disparate networks.
  ADVANTAGE - Enables selective transmission of valuable information in
manner which allows for control or replication and publication of
information.

Title Terms/Index Terms/Additional Words: DYNAMIC; CLIENT; REGISTER;
  DISTRIBUTE; INFORMATION; NETWORK; ENTITY; ORGANISE; SELECT; SHARE

Class Codes
International Classification (Main): G06F-015/00, G06F-015/16, G06F-017/30
  (Additional/Secondary): G06F-012/00, G06F-012/14, G06F-013/00
US Classification, Issued: 709203000, 709217000, 709225000, 709227000,
  709238000, 709239000, 709249000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-D01; T01-H07C5E; T01-J05B4M

  Alerting Abstract ...USE – Providing **control** over **distribution** ,
redistribution, **access** **security** , filtering, organizing and display of
information across disparate networks...

Original Publication Data by Authority

Original Abstracts:
...to resource locators directed to it and to direct the database
management program in organizing **the** dynamic client registry; several
secondary computers **networked** with the first, each having a disk for
storing a dynamic group registry and resource...

...resource locators directed to it and to direct the database management
program in organizing the **dynamic** client registry; several secondary
computers networked with the first, each having a disk for storing a
dynamic group registry and resource...

...locators directed to it and to direct the database management program in
organizing the dynamic **client** registry; several **secondary** computers
networked with the first, each having a disk for storing a dynamic group
registry and resource...
Claims:
...for execution in the client side communications server in each secondary
computer so that communications **between** the first computer and each
secondary computer cause **the** selected predetermined **functions** to be
executed dynamically in **order** to **store** and index information in the
dynamic client registry **for** selective access **by** each **secondary**
computer.

DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0009798320 - Drawing available
WPI ACC NO: 2000-087497/200007
Related WPI Acc No: 1999-561717
XRPX Acc No: N2000-068688
 Security **system for business** use **computer**
Patent Assignee: DMW WORLDWIDE INC (DMWW-N); HARTLEY B V (HART-I);
   INNERWALL INC (INNE-N); KNIGHT E (KNIG-I); MAVROS C (MAVR-I); REYNOLDS
   K (REYN-I); ZYMBALUK G (ZYMB-I)
Inventor: HARTLEY B V; KNIGHT E; MAVROS C; REYNOLDS K; ZYMBALUK G
Patent Family (5 patents, 82 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 1999066383	A2	19991223	WO 1999US13476	A	19990615	200007	B
AU 199945682	A	20000105	AU 199945682	A	19990615	200024	E
US 20020026591	A1	20020228	US 199891270	P	19980615	200220	E
			US 1999333547	A	19990615		
			US 2001834334	A	20010412		
US 6889168	B2	20050503	US 199891270	P	19980615	200531	E
			US 1999333547	A	19990615		
			US 2001834334	A	20010412		
US 20050171737	A1	20050804	US 199891270	P	19980615	200552	E
			US 1999333547	A	19990615		
			US 2001834334	A	20010412		
			US 2005100714	A	20050407		

Priority Applications (no., kind, date): US 2005100714 A 20050407; US
   2001834334 A 20010412; US 1999333547 A 19990615; US 199891270   P
   19980615

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 1999066383	A2	EN	37	15	

National Designated States,Original: AL AM AT AU AZ BA BB BG BR BY CA CH
   CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR
   KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI
   SK SL TJ TM TR TT UA UG UZ VN YU ZW
Regional Designated States,Original: AT BE CH CY DE DK EA ES FI FR GB GH
   GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW
AU 199945682   A EN   Based on OPI patent   WO 1999066383
US 20020026591   A1 EN   Related to Provisional US 199891270
                                Continuation of application US
   1999333547
US 6889168   B2 EN   Related to Provisional US 199891270
                                Continuation of application US
   1999333547
US 20050171737   A1 EN   Related to Provisional US 199891270
                                Continuation of application US
   1999333547

                                Continuation of application US
   2001834334
                                Continuation of patent US 6889168

 Alerting Abstract WO A2
   NOVELTY - Security module of the system under direction from processor
(12) accesses and analyzes selected portions of the computer comprising
unix server (10) to identify vulnerabilities. Utility module under
direction from processor performs various utility functions with regard to

computer, in response to identified vulnerabilities.
   DESCRIPTION - Security information for performing analysis of computer is
stored in security system memory (30). The security system is connected to
the computer comprising unix server (10) via (18). The reporting module of
the system provides status information to GUI with regard to operations of
the system. The security module includes at least one of configuration mode
which performs initial analysis of the **computer   system** acquire
configuration information, **directory** checking module analyzing
directories and files in system memory (13) to determine if security
initial files have been tampered, user **manager** module, integrity checking
module, **network** checking module and a password checking module. The
utility module is chosen from user manager module, file removal module,
file marking module, and scheduling module. An INDEPENDENT CLAIM is also
included for method of providing a security assessment for computer system.
   USE - For business use computer.
   ADVANTAGE - Enables manually marking certain critical files and analyzing
the marked files to detect tampering when directory check module is
activated. Enables scheduling automated performance of functions and
providing reports to the system user in a number of different formats.
   DESCRIPTION OF DRAWINGS - The figure shows block diagram of security
system.
   10 Unix server
   12 Processor
   13 System memory
   18 Via
   30 Security system memory

Title Terms/Index Terms/Additional Words: SECURE; SYSTEM; BUSINESS;
   COMPUTER
Class Codes
International Classification (Main): G06F, G06F-011/30, G06F-012/14,
   G06F-015/00
   (Additional/Secondary): H04L-009/00
US Classification, Issued: 713201000, 709224000, 702186000, 702186000,
   713201000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-H07C5A; T01-J12C

   Security **system for business** use **computer**

   Alerting Abstract ...security module includes at least one of
configuration mode which performs initial analysis of the **computer
system** acquire configuration information, **directory** checking module
analyzing **directories** and files in system memory (13) to determine if
security initial files have been tampered, user **manager** module, integrity
checking module, **network** checking module and a password checking module.
The utility module is chosen from user manager...

Original Publication Data by Authority

Original Abstracts:
...identify, notify, and possibly correct, vulnerabilities and
discrepancies. The security system includes a number of **security** tools
and **utilities in** order to **perform** these functions. The **security**
system includes the capability to identify the system configuration and
once this is done performs different processes to analyze the **computer
system directories** , locate **vulnerabilities in the** files or

directories , check the **network** **access** , do analysis **of** the users or groups which have access to the computer system and check the permissions ...

...identify, notify, and possibly correct, vulnerabilities and discrepancies. The security system includes a number of **security** tools and **utilities** in order to perform these **functions** . The **security system** includes the capability to identify the system configuration and once this is done performs different processes to analyze the **computer system directories** , locate vulnerabilities in the files or **directories** , **check** **the** **network** access, do analysis of the **users** or groups **which** have access to the **computer** **system** and check the permissions which these parties have been granted, and analyze passwords of the...

...security analysis computer system to identify, notify, and possibly correct, vulnerabilities and discrepancies. The security **system** **includes** a number of **security** tools and **utilities** in **order** to perform these functions. The security system includes **the** capability to **identify** the **system** configuration **and** once **this** is done **performs** **different** processes to analyze the **computer** **system** **directories** , locate vulnerabilities in the files or **directories** , check the **network** access, **do** **analysis** **of** the users or groups which have **access** to the **computer** **system** and check the permissions which these parties have been granted, and analyze passwords of the...

...to identify, notify, and possibly correct, vulnerabilities and discrepancies. The security system includes a number **of** security **tools** **and** **utilities** in **order** to perform these functions. The security system incudes the capability to identify the **system** configuration and **once** this **is** done **performs** **different** **processes** to analyze **the** **computer** **system** **directories** , locate vulnerabilities in the files or **directories** , check the **network** access, do analysis of the users **or** **groups** **which** have access to the **computer** system **and** **check** **the** **permissions** which these parties have been granted, and analyze passwords of the users. The utilities include...

...to permanently remove files from the computer system, mark particular files to be analyzed, as **well** as schedule the **security** tests to be performed at predetermined times...

...des vulnerabilites et des anomalies. Ce systeme de securite comporte un certain nombre d'outils **de** **securite** et d' **utilitaires** destines a executer ces fonctions. Il a la capacite d'identifier la configuration du systeme et, cela fait, d'effectuer **differentes** operations pour **analyser** les repertoires, localiser les vulnerabilites dans les fichiers ou les directoires, verifier l'acces reseau...

...permanence des fichiers du systeme, de marquer des fichiers particuliers a analyser et de planifier **les** essais de **securite** a executer a des moments predetermines.

Claims:
...said security system comprising:at least one security module which under direction from the processor **accesses** and analyzes **selected** portions of the computer apparatus to identify vulnerabilities;at least one utility module which under...
...performs various utility functions with regards to the computer apparatus in response to the identified **vulnerabilities** ; anda **security** system memory which contains security information for performing the analysis of the computer apparatus...

...**1**. A computer security system, comprising:a configuration/set-up module that operates under **direction** of a processor of a **computer system** and that identifies **security** critical **files** of the **computer system** ;a **directory** checking module that operates under **direction** of the processor and that **identifies unauthorized** changes to the security critical files; anda **user manager** module that operates **under direction** of the processor and that identifies unauthorized **access** to the **security** critical files.

...

...said security system comprising:at least one security module which under direction from the processor **accesses** and analyzes selected **portions** of the computer apparatus to identify vulnerabilities;at least one utility module which under the direction from the processor, performs various **utility** functions with **regards** to the computer apparatus in response to the identified vulnerabilities; anda security system memory

0010023825 – Drawing available
WPI ACC NO: 2000-328317/200028
XRPX Acc No: N2000-247139
**Computer system hardware resource sharing method for business application,
involves selecting at least one system operating mode and operation
interval**
Patent Assignee: SAVVY FRONTIERS PROPERTY TRUST (SAVV-N)
Inventor: WEBER H J
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 6052781	A	20000418	US 1997803636	A	19970221	200028	B

Priority Applications (no., kind, date): US 1997803636 A 19970221

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 6052781	A	EN	36	26	

Alerting Abstract US A

NOVELTY – The computer system's hardware resources are configured to
select at least one of primary and secondary system operating modes. At
least one of two operation intervals is selected during an initial ROM-BIOS
controlled POST sequence of **computer system** , preferably before BOOT
of OS.

DESCRIPTION – A computational portion, a random access memory portion and
an operator interface portion of the computer system's hardware resources
are shared between user-1 and user-2. Hard disk drive (HDD0) (90-1) and
HDD1 (90-2) are interlinked with the hardware resources. Operating system
software of user-1, user-2 are respectively maintained on HDD0 and HDD1.
The primary system operating mode enables the user-1 to access the HDD0
while denying functional access to HDD1. Secondary system operating mode
enables user-2 to access HDD1 while denying functional access to HDD0. The
operation interval includes the respective user and system operating mode.
An INDEPENDENT CLAIM is also included for the computer system hardware
resource sharing apparatus.

USE – For business and office application, for students for enabling at
least two non-current users to exercise functionally separate operational
access to hardware resources while maintaining substantially incorruptible
OS and program software integrity for each user.

ADVANTAGE – The two hard disk drives are electrically disassociated and
independently operable only by an intended user. Non-intended user cannot
access the unique hard disk drive. Even massive errors such as disk
reformat does not occur. OS on each HDD may be nearly identical or entirely
different. When the user accesses the computer system, corresponding HDD is
also accessed. Any other HDD is operationally set aside and **secured**
against **access** through password **protection** during boot by unique
removable media device or through hardware selection devices such as key
switch or user ID data card.

DESCRIPTION OF DRAWINGS – The figure shows the arrangement of PC
including operator selectable hard disk drive exclusion.
  90-1 HDD0
  90-2 HDD1

Title Terms/Index Terms/Additional Words: COMPUTER; SYSTEM; HARDWARE;
  RESOURCE; SHARE; METHOD; BUSINESS; APPLY; SELECT; ONE; OPERATE; MODE;

INTERVAL

Class Codes
International Classification (Main): G06F-013/00
US Classification, Issued: 713200000, 713002000, 713100000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-F02C2; T01-F05B2; T01-H05A

Alerting Abstract ...modes. At least one of two operation intervals is selected during an initial ROM-BIOS **controlled** POST sequence of **computer system** , preferably before BOOT of OS....computer system, corresponding HDD is also accessed. Any other HDD is operationally set aside and **secured** against **access** through password **protection** during boot by unique removable media device or through hardware selection devices such as key...

Original Publication Data by Authority

Claims:
...enables at least two non-concurrent users to exercise functionally separate operational access to the **computer system ' s hardware** resources while **maintaining** substantially **incorruptible** operating system and program software integrity for each user, comprising steps of:sharing a common...

...at least a first hard disk drive and a second hard disk drive with the **computer system** 's hardware resources; **maintaining the first** user's operating system software **and** program files on the first hard disk drive;maintaining the second user's operating system software and program **files** on the second hard disk **drive** ;configuring the **computer system** 's hardware resources to enable a selectable one of at least a first system operating...

...system operating mode, and a second interval of operation including the second user and the **second** system operating mode **during** an initial **ROM** -BIOS **controlled POST sequence** of the **computer system and** preferably prior to a BOOT of **the** operating **system.**>

DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0013129049 - Drawing available
WPI ACC NO: 2003-211125/200320
XRPX Acc No: N2003-168269
Stand-alone security **system for controlling** access to secured
information and self-service functionality for sponsor organization for
Web-based and IVR-based self-service functions
Patent Assignee: BURCHARD W (BURC-I); EDWARDS B T (EDWA-I); HARRIS S A
   (HARR-I); HUMANA INC (HUMA-N); KEINSLEY B E (KEIN-I); LATIMER E W
   (LATI-I); LAWHEAD A L (LAWH-I); LIGHT E P (LIGH-I); ROSENBERG S
   (ROSE-I); SMITHSON M A (SMIT-I); STANLEY C (STAN-I); TOWNSEND D L
   (TOWN-I); WEBER L S (WEBE-I)
Inventor: BURCHARD W; EDWARDS B T; HARRIS S A; KEINSLEY B E; LATIMER E W;
   LAWHEAD A L; LIGHT E P; ROSENBERG S; SMITHSON M A; STANLEY C; TOWNSEND D
   L; WEBER L S
Patent Family (6 patents, 100 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
WO 2003017096	A1	20030227	WO 2002US25272	A	20020812	200320	B
US 20030154403	A1	20030814	US 2001311821	P	20010814	200355	E
			US 2002216664	A	20020812		
EP 1417574	A1	20040512	EP 2002768461	A	20020812	200431	E
			WO 2002US25272	A	20020812		
AU 2002331022	A1	20030303	AU 2002331022	A	20020812	200452	E
JP 2005500617	W	20050106	WO 2002US25272	A	20020812	200505	E
			JP 2003521939	A	20020812		
IN 200400289	P4	20051209	WO 2002US25779	A	20020814	200604	E
			IN 2004CN289	A	20040212		

Priority Applications (no., kind, date): US 2002216664 A 20020812; US
   2001311821 P 20010814

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
WO 2003017096	A1	EN	176	30	

National Designated States,Original: AE AG AL AM AT AU AZ BA BB BG BR BY
   BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID
   IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ
   NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC
   VN YU ZA ZM ZW
Regional Designated States,Original: AT BE BG CH CY CZ DE DK EA EE ES FI
   FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG
   ZM ZW

US 20030154403	A1	EN			Related to Provisional US 2001311821
EP 1417574	A1	EN			PCT Application WO 2002US25272
					Based on OPI patent WO 2003017096

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI
   FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

AU 2002331022	A1	EN			Based on OPI patent WO 2003017096
JP 2005500617	W	JA	280		PCT Application WO 2002US25272
					Based on OPI patent WO 2003017096
IN 200400289	P4	EN			PCT Application WO 2002US25779

  Alerting Abstract WO A1
  NOVELTY - Sponsor organizations e.g. healthcare companies, **use** the
stand-alone **security** system for controlling **access** to **secured**
information by clients that access the company's data and other resources

over a distributed information retrieval system e.g. WWW.
  DESCRIPTION - The secured logon application is a stand-alone **security** system which controls **access** to **secured** information and self-service functionality for a sponsor organization via a secure, externally managed, dynamic menuing program that provides for controlled access to resources e.g. secured information and self-service functionality of the sponsor organization. It can be implemented using commercially available computer equipment and programming languages, and used for web-based and IVR-based self-service functions.
  USE - Web-based **security** applications for providing controlled access to sponsor organisation's data and other resources.
  ADVANTAGE - Secured logon application can have differences in configuration depending upon the sponsor organization, and can be integrated and blended into a web site between an unsecured section of the site and a secured section of the site.
  DESCRIPTION OF DRAWINGS - The drawing shows the relationship between an entity, a user, what the user can do e.g. business functions, and what data the user can perform those functions on (access identifiers).

Title Terms/Index Terms/Additional Words: STAND; SECURE; SYSTEM; CONTROL; ACCESS; INFORMATION; SELF; SERVICE; FUNCTION; ORGANISE; WEB; BASED

Class Codes
International Classification (Main): G06F-011/30, G06F-015/00, G06F-009/445
  (Additional/Secondary): G06F-015/173, G06F-017/00, G06F-017/60,
  G06F-007/00, H04L-009/00
US Classification, Issued: 713201000, 709223000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-J12C; T01-N01D1A; T01-N02B1B; T01-S01C
Stand-alone security **system for controlling** access **to** secured **information and self-service functionality for sponsor organization for Web-based and IVR-based self...**

Original Titles:
WEB-BASED **SECURITY** WITH CONTROLLED **ACCESS** TO DATA AND RESOURCES...

...WEB-BASED **SECURITY** WITH CONTROLLED **ACCESS** TO DATA AND RESOURCES...

...Web-based **security** with controlled **access** to data and resources...

...WEB-BASED **SECURITY** WITH CONTROLLED **ACCESS** TO DATA AND RESOURCES...

  Alerting Abstract ...NOVELTY - Sponsor organizations e.g. healthcare companies, **use** the stand-alone **security** system for controlling **access** to **secured** information by clients that access the company's data and other resources over a distributed...
DESCRIPTION - The secured logon application is a stand-alone **security** system which controls **access** to **secured** information and self-service functionality for a sponsor organization via a secure, externally managed, dynamic...

... **USE** - Web-based **security** applications for providing controlled access to sponsor organisation's data and other resources

Original Publication Data by Authority

Original Abstracts:

A stand-alone **security** system controlling **access** **to** **secured** information **and** self- **service** functionality for a sponsor organization, usable for Web-based and IVR-based self-service functions, having five primary facets: (1) control of **access** to **secured** information (**2**) enabling **access** to **users** having **indirect** and **direct** relationships with the **sponsor** organization (3) **distribution** of security **administration** **from** a central **information** technology resource to **users** of the **security** **system** , (4) support **for** integration into different environments, and (5) support for system integrators. Key components of access control...

...A stand-alone **security** system controlling **access** to **secured** information and self- **service** functionality for **a** sponsor **organization** , usable for Web-based and IVR-based self-service functions, having five primary facets: (1) control of **access** to **secured** information and self-service functionality for **a** sponsor **organization** , (2) enabling **access** to users having indirect relationships to the sponsor organization and to users having a **direct** relationship with the sponsor organization, (**3**) distribution of **security** **administration** from a central information technology **resource** to **various** **users** of the **security** system, (4) support for integration **into** different kinds **of** environments, and (5) support for system integrators. Key components of access control include (1) association...

...who handles day-to-day security administration for the employer. Facet (3) enables multiple levels **of** **distribution** , including enabling one organization to delegate its rights to another organization...

...A stand-alone **security** system controlling **access** to **secured** information and self-service functionality for a sponsor **organization** , usable for **Web** -based **and** IVR-based self-service functions, having five primary facets: (1) control of **access** to **secured** information (2) enabling **access** to users having indirect and **direct** relationships **with** the **sponsor** organization (3) **distribution** **of** **security** **administration** from a central **information** technology resource to **users** of the **security** system, (4) **support** for integration into different environments, and (5) **support** for system **integrators** . Key components of **access** control include (1) association of a userID with one specific person, (2) identification of keys...

...un systeme RVI et presentant cinq facettes principales: (1) surveillance de l'acces aux informations **securisees** , (2) acces aux **utilisateurs** ayant un lien indirect et **direct** avec l'organisation de parrainage, (3) distribution de **l ' administration** de **securite** **a** partir d'une ressource de **technologie** d'information centrale aux **utilisateurs** du **systeme** **securise** , (4) **support** dans le cadre de l'integration a differents environnements, (5) support aux integrateurs **de** systemes. Les **composants** cles de la surveillance de l'acces sont constitues de (1) l'association d'une...

Claims:

We claim:1. A stand-alone **security** system controlling **access** to **secured** information and self- **service** functionality for **a** sponsor **organization** , comprising:means for controlling **access** to **secured** information and self-service functionality for the sponsor **organization** ;means **for** enabling **access** to **users** who have indirect relationships to the sponsor organization as well as to users who have a **direct** relationship with the sponsor organization;means for **distributing** **security** **administration** from a **central** information technology resource to various **users** of the **security** **system** ;means **for** supporting integration into different kinds of environments; and **means** for supporting

system integrators who need to interface with and **use** **information** in the **security** system in **order** to **execute** their business **functions.**>

DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0013158471 - Drawing available
WPI ACC NO: 2003-241263/200324
Related WPI Acc No: 2003-362270
XRPX Acc No: N2003-192073
Interfacing method for security **processor** used **in online transactions over networks e.g. Internet, in which macro-** security **operations are** used **for communicating tasks and results between host and security processors**
Patent Assignee: CAVIUM NETWORKS (CAVI-N); CAVIUM NETWORKS INC (CAVI-N)
Inventor: AHMED K E; CARLSON D A; HUSSAIN M R; KESSLER R E; SANZONE R A;
  VARGA M D
Patent Family (4 patents, 33 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
EP 1282025	A2	20030205	EP 200216424	A	20020722	200324	B
JP 2003216591	A	20030731	JP 2002215500	A	20020724	200351	E
TW 576963	A	20040221	TW 2002116472	A	20020724	200455	E
US 6789147	B1	20040907	US 2001307643	P	20010724	200459	E
			US 200125512	A	20011219		

Priority Applications (no., kind, date): US 2001307643 P 20010724; US
  200125512 A 20011219

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 1282025	A2	EN	22	10	

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI
   FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

JP 2003216591	A	JA	64		
TW 576963	A	ZH			
US 6789147	B1	EN			Related to Provisional US 2001307643

Alerting Abstract EP A2
  NOVELTY - A processor includes execution units to process requests for
security operations, and output results of the requests to output data
structures associated with the requests within a remote memory based on
pointers stored in the requests.
  DESCRIPTION - The method involves communicating tasks and results between
a host processor and a security coprocessor having a number of execution
units. A host processor can transfer the type of tasks, in particular macro
security operations, to the security processor. The security coprocessor
having multiple execution units receives requests and provides results
through a continuous flow mechanism. The received requests are treated as
independent of each other, are **distributed** to available multiple
execution units in- **order** , can be macro-security **operations** , can take
different amounts of **time** to **complete** and can be **completed** /returned
out-of-order.
  INDEPENDENT CLAIMS are included for

1.a method executing on a host processor;

2.a processor including a number of execution units;

3.a system comprising a host processor coupled to a system bus;

4.a machine readable medium storing instructions for executing the

method.

USE - Processing **security** operations in online sales for business-to-**business** and **business** -to-customer over communications networks e.g. Internet.

ADVANTAGE - Macro- **security** operations can be **used** with different techniques for communicating **tasks** and results between **a** host processor and a security processor.

DESCRIPTION OF DRAWINGS - The drawing shows an exemplary establishment of a secure SSL 3.0 session according to an embodiment of the invention.

401 Client
403 Server
407,409,423,425 Security operations

Title Terms/Index Terms/Additional Words: INTERFACE; METHOD; SECURE; PROCESSOR; TRANSACTION; NETWORK; MACRO; OPERATE; COMMUNICATE; TASK; RESULT; HOST

Class Codes

International Classification (Main): G06F-001/00, G06F-015/16, G06F-009/00 (Additional/Secondary): G06F-012/00, G06F-013/00, G06F-015/177, G06F-009/38

US Classification, Issued: 710200000, 713200000, 712034000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-D01; T01-M05; T01-N01A2A; T01-N02B1B; T01-S03; W01-A05A

Interfacing method for security **processor** used **in online transactions over networks e.g. Internet, in which macro-** security **operations are** used **for communicating tasks and results between host and security processors**

Alerting Abstract ...a continuous flow mechanism. The received requests are treated as independent of each other, are **distributed** to available multiple **execution** units in- **order** , can be macro-security **operations** , can take **different** amounts of **time** to **complete** and can be **completed** /returned out-of-order...

... **USE** - Processing **security** operations in online sales for business-to- **business** and **business** -to-customer over communications networks e.g. Internet...

...ADVANTAGE - Macro- **security** operations can be **used** with different techniques for communicating **tasks** and results between **a** host processor and a security processor

Original Publication Data by Authority

Claims:
...for security operations from a host memory, wherein the number of requests are in an **order** within the host `memory ;` **distributing** , by the request unit, the **number** of requests for the security operations to a number of execution units, wherein the distribution...

...for security operations from a host memory, wherein the number of requests are in an **order** within the host memory; **distributing** , by the request unit, the number of requests for the security operations to a number of execution **units** , wherein the **distribution** is based on **availability** of the number of execution units; processing the number of

requests for the security operations...

DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0013416971 - Drawing available
WPI ACC NO: 2003-507459/200348
XRPX Acc No: N2003-403057
**Computer system operated in security trading system providing reference
market for processing orders has pre-match control unit for executing order
against quote if order matches quote**
Patent Assignee: DEUT BOERSE AG   (DEBO-N)
Inventor: GOMBER P; MAURER K; ZICKWOLFF M
Patent Family (2 patents, 27 countries)
Patent   Application
Number   Kind   Date   Number   Kind   Date   Update
EP .1321870   A1   20030625 EP 2001129858   A   20011214   200348 B
US ·20030177086 A1   20030918 US 2002307506   A   20021202   200362 E

Priority Applications (no., kind, date): EP 2001129858 A 20011214

Patent Details
Number   Kind Lan Pg Dwg Filing Notes
EP 1321870   A1   EN   28   8
Regional Designated States,Original: AL AT BE CH CY DE DK ES FI FR GB GR
   IE IT LI LT LU LV MC MK NL PT RO SE SI TR

   Alerting Abstract EP A1
   NOVELTY - A pre-match control unit (255) is used for determining whether
an order matches a quote. The pre-match control unit may be arranged for
executing the order against the quote if the order matches the quote or
automatically forwarding the order to the reference market for execution if
the order does not match the quote.
   DESCRIPTION - INDEPENDENT CLAIMS are included for:

   1.a method of operating a computer   system for processing   orders   in
     a security trading system

   USE - For processing orders in a **security** trading system providing a
reference market, in which orders are matched with quotes for execution
purposes.
   ADVANTAGE - Provides such internalization functionality without the need
to re-submit an order that could not be internalized, to the order book.
   DESCRIPTION OF DRAWINGS - The drawing illustrates a system according to a
preferred embodiment of the invention.
   255 pre-match control unit

Title Terms/Index Terms/Additional Words: COMPUTER; SYSTEM; OPERATE; SECURE
   ; TRADE; REFERENCE; MARKET; PROCESS; ORDER; PRE; MATCH; CONTROL; UNIT;
   EXECUTE

Class Codes
International Classification (Main): G06F-017/60
US Classification, Issued: 705037000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-J05A2F; T01-N01A2F

   Alerting Abstract ...a method of operating a **computer**   **system** for
processing **orders**   **in** a security **trading** system...

...USE - For processing orders in a **security** trading system providing a reference market, in which orders are matched with quotes for execution...

Original Publication Data by Authority

Original Abstracts:
The invention provides a method of operating a **computer** **system** for processing **orders** **in** a security **trading** system providing a reference market, and a corresponding computer system. A message that indicates a...

...The invention provides a method of operating a **computer** **system** for processing **orders** in a security trading **system** **providing** a reference **market**, and a corresponding **computer** **system**. A message that indicates a (private) quote is received. The quote includes quote parameters defining ...

...invention therefore provides an integrated internalization functionality in a security trading system leading to best **execution** of **orders**, to price- **time** priority consistency, order **book** consistency, full transparency and fairness.
Claims:
Computer system operated in a security trading system (260) providing a reference market, the **computer** **system** **being** **arranged** for processing **orders** and **comprising** :means for receiving a message indicating a quote, the quote including quote parameters implicitely defining...

...1. Computer system operated in a security trading system (260) providing a reference market, the **computer** **system** being arranged **for** **processing** **orders** and comprising:means for receiving a message indicating a quote, the quote including **quote** **parameters** implicitely defining a buy **limit** **order** and a sell limit order;a quote storage (250) for storing the quote parameters;means...

DIALOG(R)File 350:Derwent WPIX

0013565781 - Drawing available
WPI ACC NO: 2003-660043/200362
Related WPI Acc No: 2003-660044; 2007-024009
XRPX Acc No: N2003-526333
Data network management **and service provider using command line
interface framework, transmits command sequences to corresponding** managed
data network **entity, for execution of command line interface actions in
entity**
Patent Assignee: ALCATEL CANADA INC (COGE); CHAN D W (CHAN-I); KATZ F
  (KATZ-I); LANDRY K E D (LAND-I); MURRAY C (MURR-I); NGO C N (NGOC-I);
  ZABIHI A (ZABI-I)
Inventor: CHAN D W; KATZ F; LANDRY K E D; MURRAY C; MURRAY C W; NGO C N;
  ZABIHI A
Patent Family (7 patents, 32 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20030115304	A1	20030619	US 2002115900	A	20020405	200362	B
CA 2365436	A1	20030619	CA 2365436	A	20011219	200362	E
EP 1322066	A2	20030625	EP 2002293097	A	20021213	200362	E
US 7113989	B2	20060926	US 2002115900	A	20020405	200663	E
EP 1322066	B1	20061220	EP 2002293097	A	20021213	200702	E
DE 60216885	E	20070201	DE 60216885	A	20021213	200722	E
			EP 2002293097	A	20021213		
DE 60216885	T2	20070705	DE 60216885	A	20021213	200744	E
			EP 2002293097	A	20021213		

Priority Applications (no., kind, date): CA 2365436 A 20011219; US
  2002115900 A 20020405

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20030115304	A1	EN	13	7	
CA 2365436	A1	EN			
EP 1322066	A2	EN			

Regional Designated States,Original: AL AT BE BG CH CY CZ DE DK EE ES FI
  FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

EP 1322066	B1	EN			

Regional Designated States,Original: DE ES FR GB IT

DE 60216885	E	DE		Application EP 2002293097	
				Based on OPI patent EP 1322066	
DE 60216885	T2	DE		Application EP 2002293097	
				Based on OPI patent EP 1322066	

  Alerting Abstract US A1
  NOVELTY - A command line interface (CLI) processor (520) processes the
CLI dictionary entries holding vocabulary and grammar specifications of
commands used in interacting with at least one **managed** data **network**
entity (510), on receiving request for CLI actions to be performed from a
managed object server (MOS) (200). A communication module (540) transmits
each CLI command sequence to corresponding network entity, for execution.
  DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

  1.method of interacting with managed data network entity; and

  2.method of providing dictionary of CLI commands.

  USE - For **managing** data **networks** such as wireless local area **network**

(LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers (RAS), distribution nodes providing demultiplexing function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management** , statistics gathering, performance reporting, fault **management , network surveillance, service provisioning, billing and accounting and security enforcement using** command line interface framework.

ADVANTAGE - Provides automatic entry of CLI command in dictionary and support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network** entity **management costs and time and improves development and maintenance of the network management** and service provisioning solution.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the data **network management** and service provisioning command line interface framework.

200 managed object server
510 **managed** data **network** entity
520 CLI processor
540 communication module

Title Terms/Index Terms/Additional Words: DATA; NETWORK; MANAGEMENT; SERVICE; COMMAND; LINE; INTERFACE; FRAMEWORK; TRANSMIT; SEQUENCE; CORRESPOND; ENTITY; EXECUTE; ACTION

Class Codes
International Classification (+ Attributes)
IPC + Level Value Position Status Version

IPC	+ Level	Value	Position	Status	Version
G06F-0015/173	A	I	F	B	20060101
H04L-0012/24	A	I		R	20060101
H04L-0012/24	A	I	F	B	20060101
H04L-0012/24	A	I	F		20060101
G06F-0015/16	C	I	F	B	20060101
H04L-0012/24	C	I		R	20060101
H04L-0012/24	C	I	F	B	20060101
H04L-0012/24	C	I			20060101
H04L-0012/24	C	I		B	20060101

US Classification, Issued: 709223000, 709222000, 709224000, 709220000, 709223000, 370241000, 370254000, 707100000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-F05B; T01-N02A2; W01-A06B5A; W01-A06E

Data network management **and service provider using command line interface fr**amework, transmits command sequences to corresponding managed **data** network **entity, for execution of command line interface actions in entity**

Alerting Abstract ...entries holding vocabulary and grammar specifications of commands used in interacting with at least one **managed** data **network** entity (510), on receiving request for CLI actions to be performed from a managed object...
...method of interacting with **managed** data **network** entity; and method of providing dictionary of CLI commands...

...USE - For **managing** data **networks** such as wireless local area **network** (LAN) comprising data switching equipments, routers, bridge, access nodes providing multiplexing function, remote access servers...

...function, customer premise equipment (CPE) and for controlling software applications such as inventory reporting, configuration **management ,** statistics gathering, performance reporting, fault **management , network** surveillance, service provisioning, billing and accounting and **security enforcement using** command line interface framework...

...support for multi-vendor equipment by using multiple CLI command vocabularies and dictionaries. Reduces data **network** entity **management** costs and time and improves development and maintenance of the **network management** and service provisioning solution...

...DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the data **network management** and service provisioning command line interface framework...
...510 **managed** data **network** entity...

Original Publication Data by Authority

Original Abstracts:
A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved form a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved form a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...

...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...
...commands in the CLI command sequence are sent for execution. The

solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing **network** **management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network** **management** and service provisioning solution...

...A method of interacting with a **managed** data **network** entity is provided. The method includes a sequence of steps. A change in the operational state of the **managed** data **network** entity is detected. A CLI dictionary entry is retrieved form a CLI dictionary associated with...

...Based on the retrieved CLI dictionary entry, CLI commands are extracted therefrom to configure the **managed** data **network** entity to reflect the detected change in the operational state. A CLI command sequence is...
...the extracted CLI commands. Each CLI command in the command sequence is sent to the **managed** data **network** entity for execution. CLI command responses are monitored. Based on a successful execution of CLI...

...commands in the CLI command sequence are sent for execution. The solution provides automated configuration **management** of data **network** entities from different vendors when SNMP is not a viable option. The automation eliminates manual CLI command entry in providing network **management** and service provisioning solutions, provides support for multi-vendor equipment by processing multiple CLI command vocabulary and grammar specifications in the CLI command dictionary. The solution reduces data **network** entity **management** costs, downtime, and training time for analysts. The advantages are derived from the ability to...

...data network entities with human readable code greatly improving the development and maintenance of the **network** **management** and service provisioning solution.
Claims:
    Network **management** and service provisioning Command Line Interface (CLI) framework, comprising: a. a processor responsive to...

...holding vocabulary and grammar specifications of a plurality of commands used in interacting with at **least** one **managed** data network entity; and c. a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries** **wherein** a network management and service provisioning solution is provided making abstraction of the **at** least **one** managed data network entity...

...A Command Line Interface (CLI) **framework** **for** a network **manager** (NM) that manages **a** plurality of managed entities **of** a communication network, comprising: a CLI dictionary (530) holding vocabulary and grammar specifications for all...

...sequence of commands required to configure a managed entity that said managed object represents in **response** to **said** **event** and handling **execution** of **said** sequence of commands at said managed entity; anda communications module (540) for transmitting said sequence of commands to

said managed entity for execution, and interpreting results **received** from said managed **entity ,** **wherein** a network management and service provisioning solution is provided making abstraction of the type of...

...I/we **claim** : 1 . A network management and service provisioning Command Line Interface (CLI) framework, comprising: a. a processor...

...entries holding vocabulary and grammar specifications of a plurality of commands used in interacting with **at** least **one** managed data network entity; and c. a communications module sending in sequence for execution and...

...of commands generated in response to the notification as specified in the plurality of dictionary **entries** **wherein** a network management and service provisioning solution is provided making abstraction of the **at** least **one** managed data network entity...

...We claim:1. A Command Line Interface (CLI) framework **component** **of** a Network Management System (**NMS**), the NMS managing a plurality **of** field **installed** managed communications network entities **of** a communications network, **each** field **installed** managed communications network entity being represented and modeled by an associated managed object instance stored...

...database associated with the NMS, the CLI framework component comprising: a. a CLI dictionary codifying **a** plurality **of** managed communications network entity-specific **CLI** commands and maintaining at least one **mapping** between **the** managed communications network entity-specific CLI commands **and** a corresponding managed object type;b. a generic processor executing coded logic to: i. detect...

...responsive to the detected event selectively generate a sequence of CLI commands required to configure **the** field **installed** managed communications network entity **associated** with said managed object instance by consulting the CLI dictionary;iii. handle execution of said sequence of CLI commands at **said** field **installed** managed communications network entity, including interpreting CLI command execution results received from **said** field **installed** managed communications network entity; andiv. generating an error report based on an unsuccessful execution...

...the execution results; andc. a communications module transmitting said sequence of CLI commands to **said** field **installed** managed communications network entity to be executed thereon, and conveying the execution results received from **said** field **installed** managed communications network entity to the generic **processor ,** **wherein** a network management and service provisioning solution is provide **making** abstraction **of** managed communications network entity types.

```
Set       Items    Description
S1      1569864    COMPUTER?(2N)SYSTEM? ? OR NETWORK? OR DISTRIBUT? OR ETHERN-
                   ET? OR INTERNET OR INTRANET? OR LAN OR LANS OR WAN OR WANS OR
                   WLAN? ? OR VLAN? ?
S2        14742    S1(5N)(PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD? -
                   OR ENFORC?)(3N)(ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UT-
                   ILI? OR USING)
S3         3481    S2(5N)(ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG?
                   OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPE-
                   RVIS???)
S4       195926    (ORDER?()SET? ? OR SEQUEN? OR PATTERN? OR ORDER?)(5N)(LEVE-
                   L? OR STEP? ? OR STAGE? OR TIER?? ? OR OPERATION? OR FUNCTION?
                   OR COMMAND?)
S5        26666    S4(5N)(TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO-
                   N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR
                   MINUTE? ? OR SECOND? ? OR PERIOD?)
S6        33021    S4:S5(5N)(SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE
                   OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADD-
                   ITIONAL)
S7         5876    S6(5N)(PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR -
                   OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?)()OUT OR
                   COMPLET? OR ENABL? OR ALLOW?)
S8        54114    (PRESELECT? OR PRE()SELECT? OR (SELECT? OR PICK??? OR CHOO-
                   SE? OR DESIGNAT? OR CHOSEN OR IDENT?)()BEFORE? OR PREDETERMIN?
                   OR PRE()(DETERMIN? OR SPECIF?))(5N)(ACCESS? OR ENTRY OR ENTR-
                   IE? ? OR USE??? OR UTILI?)
S9            1    S3 AND S7 AND S8
S10         126    S3 AND ENFORC?(3N)SECUR?
S11           3    S10 AND S8
S12           2    S2:S3 AND S7 AND S8
S13           1    S12 NOT (S9 OR S11)
S14          22    S2:S3 AND S4:S5 AND S8
S15          19    S14 NOT (S9 OR S11:S13)
S16      126817    (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
                   RANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?)(5N)(-
                   SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUER-
                   IE? ? OR REQUEST? OR ASK???)
S17      274804    (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
                   DOWNLOAD? OR FETCH??? OR ACCESS?)(5N)(SEARCH? OR RESEARCH? OR
                   RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK-
                   ???)
S18           4    S15 AND S16:S17
S19          15    S15 NOT S18
S20          13    AU=(KOVARIK V? OR KOVARIK, V?)
S21           0    (VINCENT OR VINCE OR VINNIE)(2N)KOVARIK
S22           1    S20 AND S2:S3
File 350:Derwent WPIX 1963-2007/UD=200752
         (c) 2007 The Thomson Corporation
File 347:JAPIO Dec 1976-2007/Mar(Updated 070809)
         (c) 2007 JPO & JAPIO
```

Abstract fat files (2)

11/69,K/1   (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0015307045 - Drawing available
WPI ACC NO: 2005-657227/200567
XRPX Acc No: N2005-538483
**Secure access method in computer system, involves granting access request
only, if access request does not complete prohibited temporal access
pattern and minimum access level for base node does not exceed**
predetermined   access **level**
Patent Assignee: HARRIS CORP   (HARO)
Inventor: KOVARIK V J
Patent Family (5 patents, 40 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20050204131	A1	20050915	US 2004798074	A	20040311	200567	B
CA 2499986	A1	20050911	CA 2499986	A	20050309	200567	E
EP 1577735	A2	20050921	EP 20055394	A	20050311	200567	E
JP 2005259146	A	20050922	JP 200565879	A	20050309	200567	E
CN 1667544	A	20050914	CN 200510054559	A	20050311	200607	E

Priority Applications (no., kind, date): US 2004798074 A 20040311

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20050204131	A1	EN	18	10	
CA 2499986	A1	EN			
EP 1577735	A2	EN			

Regional Designated States,Original: AL AT BA BE BG CH CY CZ DE DK EE ES
   FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU

| JP 2005259146 | A | JA | 17 | | |

Alerting Abstract US A1
   NOVELTY - The method involves determining if **access** request from entity
with **predetermined** **access** level, completes a prohibited temporal access
pattern for entity. A minimum access level established for base node (110)
is compared to **predetermined** **access** level. The **access** request is
granted only, if the access request does not complete the access pattern
and minimum **access** level does not exceed **predetermined** **access** level.
   DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

   1.method for restricting access to computer system; and

   2.computer system.

   USE - For secure access computer system.
   ADVANTAGE - Enables maintaining the access authorities for each user
dynamically, thereby allowing system objects to have multiple level of
access classification based on historical access by each user.
   DESCRIPTION OF DRAWINGS - The figure shows the data primitives and
hierarchical graph for secure access to computer system.
   1021-1024 object types
   1041-1043 system functions
   110 base node
   112 higher level node

Title Terms/Index Terms/Additional Words: SECURE; ACCESS; METHOD; COMPUTER;
   SYSTEM; REQUEST; COMPLETE; PROHIBIT; TEMPORAL; PATTERN; MINIMUM; LEVEL;
   BASE; NODE; PREDETERMINED

Class Codes
International Classification (Main): G06F-001/00, G06F-012/14, H04L-009/00
US Classification, Issued: 713166000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-H01C2; T01-J12C; T01-N02B1B; W01-A06E1C

...complete prohibited temporal access pattern and minimum access level for base node does not exceed predetermined access **level**

Original Titles:
...Method and **system enforcing computer security utilizing** an adaptive lattice mechanism...

... **ENFORCING** COMPUTER **SECURITY** UTILIZING ADAPTIVE LATTICE MECHANISM...

... **Enforcing** computer **security** utilizing an adaptive lattice mechanism
    ...NOVELTY - The method involves determining if **access** request from entity with **predetermined access** level, completes a prohibited temporal access pattern for entity. A minimum access level established for base node (110) is compared to **predetermined access** level. The **access** request is granted only, if the access request does not complete the access pattern and minimum **access** level does not exceed **predetermined access** level.

Original Publication Data by Authority

Original Abstracts:
...the computer system a request from an entity (using 1002). The entity can have a **predetermined access** authorization level **for access** to a first **base** node (110) representing an information type (102) or a computer system function (104). The system...

...access pattern for the entity. The system also compares a minimum access level established for **the** first base node to the **predetermined access** authorization level `assigned to` the entity. Thereafter, the system can grant the access request only if the minimum access level for the first base node does not exceed to the **predetermined access** authorization level.

    ...

...the computer system a request from an entity (using 1002). The entity can have a **predetermined access** authorization level for **access** to a first base node (110) representing **an information** type (102) or **a** computer system function (104). The system determines if the access request completes a prohibited temporal...

...entity. The system also compares a minimum access level established for the first base node **to** the **predetermined access** authorization level assigned to the entity. Thereafter, the system can grant the **access** request only if the **minimum access** level for the first base node does not exceed to the **predetermined access** authorization level.
Claims:
...the steps of:receiving in said computer system a request from an entity with a **predetermined access** level for **access to** a first **base** node representing at least one of an information type and a computer system function;determining...

...for said entity; andcomparing a minimum access level established for said first base node **to** said **predetermined** **access** level; andgranting said **access** request **only** **if** it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed **said** **predetermined** **access** level.

...

...computer system, comprising the steps of:receiving in said computer system a request from an **entity** with a **predetermined** **access** level for **access** to a first base node representing at least one of an information type and a **computer** **system** function;determining **if** said **access** request completes a prohibited temporal access pattern for said entity; andcomparing a minimum access level established for said first base **node** to said **predetermined** **access** level; **and** granting said **access** request only if it does not complete a prohibited temporal access pattern for said entity, and said **minimum** **access** level for said first base node **does** not exceed said **predetermined** **access** level.

13/69,K/1   (Item 1 from file: 350)

0001862168
WPI ACC NO: 1979-K8815B/197947
**Authenticating identity of user of information system - transferring
terminal user authentication pattern with identification number to host
data processing system**
Patent Assignee: IBM CORP   (IBMC)
Inventor: MATYAS S M; MEYER C H W
Patent Family (5 patents, 5 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
EP 5179	A	19791114	EP 1979101038	A	19790405	197947	B
US 4218738	A	19800819	US 1978903286	A	19780505	198036	E
CA 1111563	A	19811027				198148	E
EP 5179	B	19830518	EP 1979101038	A	19790405	198321	E
DE 2965420	G	19830707				198328	E

Priority Applications (no., kind, date): EP 1979101038 A 19790405; US
  1978903286 A 19780505

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
EP 5179	A	EN			
Regional Designated States,Original: DE FR GB IT					
CA 1111563	A	EN			
EP 5179	B	EN			
Regional Designated States,Original: DE FR GB IT					

  Alerting Abstract EP A
  A process confirms the identity of a terminal user provided with an
identification number and a secret password in a system providing data
communication between a terminal and a host data processing system each
having cryptographic appts. The identification number and password are used
at the terminal to obtain a terminal user authentication pattern which is
transferred with the identification number from the terminal to the host
d.p.s.
  At the host d.p.s. an operation is performed in accordance with a
predetermined number provided by the host and the terminal user
identification number to obtain a terminal user first verification pattern.
The latter is compared with a second verification pattern obtained at the
host d.p.s. in accordance with a **predetermined** terminal **user** test
pattern provided at the host d.p.s. and the terminal user authentication
pattern.
  The process authenticates the identity of a terminal user provided with
an identification number and a secret password more securely than
customary.

Title Terms/Index Terms/Additional Words: AUTHENTICITY; IDENTIFY; USER;
  INFORMATION; SYSTEM; TRANSFER; TERMINAL; PATTERN; NUMBER; HOST; DATA;
  PROCESS

Class Codes
International Classification (Main): G06F-013/00
 (Additional/Secondary): G06F-003/00, G07C-011/00, H04K-001/00
US Classification, Issued: 380025000, 340825310, 364DIG002, 364222200,
  364222500, 364228400, 364234000, 364235000, 364236200, 364236300,
  364238300, 364248100, 364248200, 364259000, 364259200, 380045000

File Segment: EPI;
DWPI Class: T01; T05

Alerting Abstract ...a second verification pattern obtained at the host d.p.s. in accordance with a **predetermined** terminal **user** test pattern provided at the host d.p.s. and the terminal user authentication pattern...

Original Publication Data by Authority

Original Abstracts:
...authentication processing. This is accomplished by providing terminal user identification numbers and passwords and a **predetermined** **number** at the host data processing system. A first initialization operation is performed at the host...

...in accordance with the terminal user identification numbers and passwords to obtain terminal user authentication **patterns** .A **second** initialization **operation** is **performed** at **the** host **data** processing **system** in **accordance** with the **predetermined** number and the terminal **user** identification numbers **to** obtain terminal **user** first **verification** patterns. A third initialization operation is performed at the host data processing system in accordance...

...during authentication processing and for generating test patterns during the secure run is disclosed which **uses** a variation of the host computer master **key** to reduce risk of **compromise** of total **system** **security** . The **use** of a variant of the host master key prevents system programmers and/or computer operators...
?

DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0016174489 - Drawing available
WPI ACC NO: 2006-706129/200673
XRPX Acc No: N2006-555460
 Security **apparatus for** use **in telecommunication** system , **has** computer
 for providing user **authorization by comparing authorization user input**
to security code based on retrieved **user profile**
Patent Assignee: ACCESSLINE COMMUNICATIONS CORP (ACCE-N)
Inventor: EPLER F A; KNIGHT J M; STENSBERG P A; ZHUK O V
Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 7106845	B1	20060912	US 2000604283	A	20000626	200673	B

Priority Applications (no., kind, date): US 2000604283 A 20000626

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 7106845	B1	EN	27	11	

   Alerting Abstract US B1
   NOVELTY - The apparatus has a database storing a user profile indicating
a set of security modes selectable by the user. A computer communicates
with the database to receive telecommunication data transmissions. The
computer stores selected security mode in the user profile corresponding to
the user. The computer provides user authorization by comparing
authorization user input to a security code based on the **retrieved** user
profile.
   DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

   1.a method of providing security for a telecommunication system

   2.a computer-readable signal bearing medium storing instructions for a
     computer for providing security for a telecommunication system

   3.a user prompt signal for providing security for a telecommunication
     system.

   USE - Used in a telecommunication system for telecommunication company,
professional service provider such as doctor, lawyer and accountant,
financial institution such as bank and securities broker and insurance
company.
   ADVANTAGE - The computer compares the authorization user input to the
security code based on the **retrieved** user profile to provide user
authorization, thus effectively providing user security and access to the
telecommunication system.
   DESCRIPTION OF DRAWINGS - The drawing shows a block diagram of a suitable
environment employing a dynamic security system.

Title Terms/Index Terms/Additional Words: SECURE; APPARATUS;
   TELECOMMUNICATION; SYSTEM; COMPUTER; USER; AUTHORISE; COMPARE; INPUT;
   CODE; BASED; **RETRIEVAL** ; PROFILE

Class Codes
International Classification (+ Attributes)
IPC + Level Value Position Status Version
  H04M-0003/42 A I F B 20060101

US Classification, Issued: 379207110, 379201120, 379189000, 455410000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-N02B1B; T01-S03; W01-A05B; W01-C02B6

Security **apparatus for** use **in telecommunication** system , **has** computer **for providing** user **authorization by comparing authorization user input to security code based on** retrieved **user profile**

Alerting Abstract ...provides user authorization by comparing authorization user input to a security code based on the **retrieved** user profile....ADVANTAGE - The computer compares the authorization user input to the security code based on the **retrieved** user profile to provide user authorization, thus effectively providing user security and access to the ...

Title Terms.../Index Terms/Additional Words: **RETRIEVAL** ;

Original Publication Data by Authority

Original Abstracts:
...typically only the user would know. Another level of security employs voice fingerprinting or voice **pattern** recognition. Yet another **level** employs a N by M matrix of random numbers, from which a **user** selects numbers from **predetermined** positions to generate a current security code. Various levels of security may be performed on...
Claims:
...user profile corresponds to the user, in response to a telecommunications call from the user, **retrieve** the at least one user profile, receive authorization user input, and provide user authorization by comparing the received authorization user input to a security code based on the **retrieved** user profile, wherein the security code is an automatically and dynamically generated user security code...

...wherein the plurality of security modes includes a current time sequence recognition mode wherein the **user** security code is based on **predetermined** numerical sequence based on an hour of day, day of week, day of month and...

22/69,K/1   (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0015307045 - Drawing available
WPI ACC NO: 2005-657227/200567
XRPX Acc No: N2005-538483
 Secure   access   **method in** computer   system , **involves granting** access
**request only, if access request does not complete prohibited temporal
access pattern and minimum access level for base node does not exceed
predetermined access level**
Patent Assignee: HARRIS CORP   (HARO)
Inventor: **KOVARIK V J**
Patent Family (5 patents, 40 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
US 20050204131	A1	20050915	US 2004798074	A	20040311	200567	B
CA 2499986	A1	20050911	CA 2499986	A	20050309	200567	E
EP 1577735	A2	20050921	EP 20055394	A	20050311	200567	E
JP 2005259146	A	20050922	JP 200565879	A	20050309	200567	E
CN 1667544	A	20050914	CN 200510054559	A	20050311	200607	E

Priority Applications (no., kind, date): US 2004798074 A 20040311

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20050204131	A1	EN	18	10	
CA 2499986	A1	EN			
EP 1577735	A2	EN			

Regional Designated States,Original: AL AT BA BE BG CH CY CZ DE DK EE ES
   FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU

JP 2005259146	A	JA	17		

  Alerting Abstract US A1
  NOVELTY - The method involves determining if access request from entity
with predetermined access level, completes a prohibited temporal access
pattern for entity. A minimum access level established for base node (110)
is compared to predetermined access level. The access request is granted
only, if the access request does not complete the access pattern and
minimum access level does not exceed predetermined access level.
  DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

  1.method for restricting access to computer system; and

  2.computer system.

  USE - For **secure access computer system** .
  ADVANTAGE - Enables maintaining the access authorities for each user
dynamically, thereby allowing system objects to have multiple level of
access classification based on historical access by each user.
  DESCRIPTION OF DRAWINGS - The figure shows the data primitives and
hierarchical graph for **secure access** to **computer system** .
  1021-1024 object types
  1041-1043 system functions
  110 base node
  112 higher level node

Title Terms/Index Terms/Additional Words: SECURE; ACCESS; METHOD; COMPUTER;
  SYSTEM; REQUEST; COMPLETE; PROHIBIT; TEMPORAL; PATTERN; MINIMUM; LEVEL;
  BASE; NODE; PREDETERMINED

Class Codes
International Classification (Main): G06F-001/00, G06F-012/14, H04L-009/00
US Classification, Issued: 713166000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-H01C2; T01-J12C; T01-N02B1B; W01-A06E1C

Secure access **method in** computer system , **involves granting** access
request only, if access request does not complete prohibited temporal
access pattern and minimum access...

Original Titles:
...Method and **system enforcing computer security utilizing** an
adaptive lattice mechanism...
Inventor: **KOVARIK V J**

Alerting Abstract ... **USE** - For **secure access computer system** .
. . .

...DESCRIPTION OF DRAWINGS - The figure shows the data primitives and
hierarchical graph for **secure access** to **computer system** .

Original Publication Data by Authority

Inventor name & address:
 KOVARIK V J ...

... **Kovarik, Vincent Joseph, Jr** ...

... **KOVARIK VINCENT JOSEPH JR** ...

... **Kovarik, Vincent Joseph JR**
Original Abstracts:
Method and apparatus for ensuring **secure access** to a **computer system**
 (1000). The **method can** begin with the step of receiving in the
computer system a request from an entity...

...Method and apparatus for ensuring **secure access** to a **computer**
system (1000). The method **can** ᐟ**begin** with the **step of**
receiving in the **computer system** a request from an entity (**using**
1002). The entity can have a predetermined access authorization
level for access to a first...
Claims:
A method for **secure access to a computer system , comprising**
the steps of:receiving in said computer system a request from an entity
with a predetermined...

...1. A method for **secure access** to a **computer system ,**
comprising the steps of:receiving in said **computer system** a request
from. **an entity** with a **predetermined access** level for · **access** to a
first base node representing at least one of an information type and a...
?

```
Set     Items   Description
S1      883612  COMPUTER?(2N)(SYSTEM? ? OR SECUR?) OR NETWORK? OR DISTRIBU-
                T? OR ETHERNET? OR INTERNET OR INTRANET? OR LAN OR LANS OR WAN
                OR WANS OR WLAN? ? OR VLAN? ?
S2       14705  S1(7N)((PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD?-
                )(5N)(ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI? OR US-
                ING))
S3        3588  S2(7N)(ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG?
                OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPE-
                RVIS???)
S4      374666  (ORDER?()SET? ? OR SEQUEN? OR PATTERN? OR ORDER?OR SEQUENT-
                IAL? OR  SERIE?? OR SERIAL?? OR IN()ORDER? OR CONTIGU? OR  CO-
                NSECUT? OR SERIAT? OR STEPWISE? OR CONSECUT? OR ONE()AFTER(2W-
                )(OTHER OR ANOTHER))(5N)(LEVEL? OR STEP? ? OR STAGE? OR TIER??
                ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S5       47231  S4(5N)(TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO-
                N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR
                MINUTE? ? OR SECOND? ? OR PERIOD?)
S6       90467  S4:S5(7N)(SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE
                OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADD-
                ITIONAL)
S7       17781  S6(7N)(PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR -
                OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?)()OUT OR
                COMPLET? OR ENABL? OR ALLOW?)
S8       70957  (PRESELECT? OR PRE()SELECT? OR (SELECT? OR PICK??? OR CHOO-
                SE? OR DESIGNAT? OR CHOSEN OR IDENT?)()BEFORE? OR PREDETERMIN?
                OR PRE()(DETERMIN? OR SPECIF?))(5N)(ACCESS? OR ENTRY OR ENTR-
                IE? ? OR USE??? OR UTILI?)
S9      101478  (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
                RANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?)(5N)(-
                SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUER-
                IE? ? OR REQUEST? OR ASK???)
S10     211155  (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
                DOWNLOAD? OR FETCH??? OR ACCESS?)(5N)(SEARCH? OR RESEARCH? OR
                RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK-
                ???)
S11          6  S2:S3(100N)S7(100N)S8(100N)S9:S10
S12         15  S2:S3(100N)S4:S5(100N)S8(100N)S9:S10
S13         18  S11:S12
S14          5  AU=(KOVARIK V? OR KOVARIK, V?)
S15          3  (VINCENT OR VINCE OR VINNIE)(2N)KOVARIK
S16          0  S14:S15(100N)S1(100N)S2:S3
S17          0  S14:S15(100N)S4(100N)S8(100N)S9:S10
S18          0  S14:S15(100N)S1
File 348:EUROPEAN PATENTS 1978-2007/ 200732
         (c) 2007 European Patent Office
File 349:PCT FULLTEXT 1979-2007/UB=20070809UT=20070802
         (c) 2007 WIPO/Thomson
```

FullTextPat.files

(DIALOG(R)File 349:PCT FULLTEXT)

00571474   **Image available**
COMPUTER NETWORK INTRUSION DETECTION
DETECTION D'INTRUSION DANS UN RESEAU INFORMATIQUE
Patent Applicant/Assignee:
  VISA INTERNATIONAL SERVICE ASSOCIATION,
  DIEP Thanh A,
Inventor(s):
  DIEP Thanh A,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 200034847 A1 20000615 (WO 0034847)
  Application: WO 99US29080 19991207 (PCT/WO US9929080)
  Priority Application: US 98208617 19981208
Designated States:
(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)
  AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB
  GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD
  MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG
  US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU
  TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG
  CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class (v7): G06F-001/00
Publication Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 11423

English Abstract
  Detecting harmful or illegal intrusions into a computer network or into
  restricted portions of a computer network uses statistical analysis to
  match user commands and program names with a template sequence. Discrete
  correlation matching and permutation matching are used to match
  sequences. The result of the match is input to a feature builder and then
  a modeler to produce a score. The score indicates possible intrusion. A
  sequence of user commands and program names and a template sequence of
  known harmful commands and program names from a set of such templates are
  retrieved. A closeness factor indicative of the similarity between the
  user command sequence and a template sequence is derived from comparing
  the two sequences. The user command sequence is compared to each template
  sequence in the set of templates thereby creating multiple closeness or
  similarity measurements. These measurements are examined to determine
  which sequence template is most similar to the user command sequence. A
  frequency feature associated with the user command sequence and the most
  similar template sequence is calculated. It is determined whether the
  user command sequence is a potential intrusion into restricted portions
  of the computer network by examining output from a modeler using the
  frequency feature as one input.

French Abstract
  L'invention concerne la detection d'intrusions nuisibles ou illegales
  dans un reseau informatique ou dans des parties reservees dudit reseau,
  qui consiste a utiliser des analyses statistiques pour comparer des
  commandes d'utilisateur et des noms de programmes a une sequence modele.
  Une correspondance de correlation et une correspondance de permutation
  discretes servent a comparer des sequences. Le resultat de la
  correspondance est introduit dans un realisateur de caracteristiques,

puis dans un modeliseur pour etablir une cote, laquelle permet d'indiquer
une intrusion possible. Une sequence de commandes d'utilisateur et de
noms de programmes, ainsi qu'une sequence modele de commandes et de noms
de programmes nuisibles provenant de tels modeles sont recherchees. Un
facteur de proximite, indiquant la similitude entre la sequence de
commandes d'utilisateur et la sequence modele, est deduit de la
comparaison des deux sequences. La sequence de commandes d'utilisateur
est comparee a chaque sequence modele de l'ensemble de modeles. On
etablit ainsi plusieurs mesures de proximite ou de similitude. L'examen
de ces mesures permet de determiner la sequence modele qui presente le
plus de similitudes avec la sequence de commandes d'utilisateur. Une
caracteristique de frequence, associee a la sequence de commandes
d'utilisateur et a la sequence modele qui presente le plus de
similitudes, est calculee. On determine si la sequence de commandes
d'utilisateur constitue une intrusion potentielle dans des parties
reservees du reseau informatique en examinant le resultat d'un modeliseur
au moyen de la caracteristique de frequence en tant qu'une entree.

Fulltext Availability:
  Detailed Description

Detailed Description
... set of templates is created and can be added to whenever a newly
  identified suspicious **command** sequence is discovered. The process of
  generating templates of command sequences is then complete.

  Related...

...is analyzed, the program selects the first template from
  1 4
  template set 14, and **retrieves** the next template in the second
  iteration, as described below in step 5 1 0...

...Y selection can be based on other criteria such as frequency,
  importance, or length.

  At **step** 506 input **sequence** X ...input sequence X`being analyzed
  1 5
  as shown in FIG. 5. Template Y' is **retrieved** at step 602. Examples of
  other features are the number of audit records processed for...

...all sequences entered by the same user during time period T. Preferably,
  the duration of **time** period T used in this **step** is greater than the
  sequence length of the input **sequence** from **step** 306.

  io Thus, if the user input **sequence** contains **commands** and program
  names entered by a user over 30 minutes, time period T is preferably...

...program to calculate an average occurrence or frequency level
  dynamically without having to store and **retrieve** from memory the
  multiple values that would be needed to calculate a static average. A...

```
Examination:        051130 A2 Date of request for examination: 20051005
Change:             060517 A2 Title of invention (German) changed: 20060517
Change:             060517 A2 Title of invention (English) changed: 20060517
Change:             060517 A2 Title of invention (French) changed: 20060517
Change:             061213 A2 Title of invention (German) changed: 20061213
Change:             061213 A2 Title of invention (English) changed: 20061213
Change:             061213 A2 Title of invention (French) changed: 20061213
Grant:              070516 B1 Granted patent
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text   Language    Update     Word Count
        CLAIMS A  (English)   200442       575
        CLAIMS B  (English)   200720       404
        CLAIMS B   (German)   200720       390
        CLAIMS B   (French)   200720       436
        SPEC A    (English)   200442       6252
        SPEC B    (English)   200720       5715
Total word count - document A              6828
Total word count - document B              6945
Total word count - documents A + B        13773
```

...SPECIFICATION phone carried by the user exists in registered specific
area where the user makes a **request** for a video information
distribution service to be provided and the traffic of the radio channel
connected to the mobile phone carried by the **user** is lower than the
predetermined threshold, video information about the specific area is
distributed from the video contents server to the mobile phone based on
push technology, so that the **user** can **securely** be **distributred**
with, for example, video information of commercial, guidance or the like
about the specific area...

...a predetermined time period, but displaying the distributed video
information is restricted within the predetermined **time** **in** **order** to
prevent the **function** of the mobile phone from be occupied with
displaying the distributed video information. After the...

...SPECIFICATION phone carried by the user exists in registered specific
area where the user makes a **request** for a video information
distribution service to be provided and the traffic of the radio channel
connected to the mobile phone carried by the **user** is lower than the
predetermined threshold, video information about the specific area is
distributed from the video contents server to the mobile phone based on
push technology, so that the **user** can **securely** be **distributred**
with, for example, video information of commercial, guidance or the like
about the specific area...

...a predetermined time period, but displaying the distributed video
information is restricted within the predetermined **time** **in** **order** to
prevent the **function** of the mobile phone from be occupied with
displaying the distributed video information. After the...

```
Set      Items    Description
S1    12454539   COMPUTER?(2N)(SYSTEM? ? OR SECUR?) OR NETWORK? OR COMPUTER?
                 OR DISTRIBUT? OR ETHERNET? OR INTERNET OR INTRANET? OR LAN OR
                 LANS OR WAN OR WANS OR WLAN? ? OR VLAN? ?
S2       22262   S1(7N)((PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD?-
                 )(5N)(ACCESS? OR ENTRY? OR ENTRIE? ? OR ENTREE? OR USE??? OR -
                 UTILI? OR USING))
S3        6211   S2(7N)(ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG?
                 OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPE-
                 RVIS???)
S4      475945   (ORDER?()SET? ? OR SEQUEN? OR PATTERN? OR ORDER?OR SEQUENT-
                 IAL?' OR  SERIE?? OR SERIAL?? OR IN()ORDER? OR CONTIGU? OR  CO-
                 NSECUT? OR SERIAT? OR STEPWISE? OR CONSECUT? OR ONE()AFTER(2W-
                 )(OTHER OR ANOTHER))(5N)(LEVEL? OR STEP? ? OR STAGE? OR TIER??
                 ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S5       38489   S4(5N)(TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO-
                 N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR
                 MINUTE? ? OR SECOND? ? OR PERIOD?)
S6       64248   S4:S5(7N)(SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE
                 OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADD-
                 ITIONAL)
S7        5797   S6(7N)(PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR -
                 OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?)()OUT OR
                 COMPLET? OR ENABL? OR ALLOW?)
S8        4102   (PRESELECT? OR PRE()SELECT? OR (SELECT? OR PICK??? OR CHOO-
                 SE? OR DESIGNAT? OR CHOSEN OR IDENT?)()BEFORE? OR PREDETERMIN?
                 OR PRE()(DETERMIN? OR SPECIF?))(5N)(ACCESS? OR ENTRY OR ENTR-
                 IE? ? OR USE??? OR UTILI?)
S9      144801   (DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT? OR T-
                 RANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?)(5N)(-
                 SEARCH? OR RESEARCH? OR RETRIEV? OR INQUIR? OR QUERY? OR QUER-
                 IE? ? OR REQUEST? OR ASK???)
S10     489980   (RETRIEV? OR RECEIV??? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR
                 DOWNLOAD? OR FETCH??? OR ACCESS?)(5N)(SEARCH? OR RESEARCH? OR
                 RETRIEV? OR INQUIR? OR QUERY? OR QUERIE? ? OR REQUEST? OR ASK-
                 ???)
S11          0   S2:S3 AND S7 AND S8
S12          1   S2:S3 AND S4:S5 AND S8
S13          0   S7 AND S8 AND S9:S10
S14        150   AU=(KOVARIK V? OR KOVARIK, V?)
S15          0   (VINCENT OR VINCE OR VINNIE)(2N)KOVARIK
S16         21   S14 AND S1:S3
S17          0   S16 AND S4 AND S8
S18          0   S16 AND S9:S10
S19         15   RD S16   (unique items)
File     2:INSPEC 1898-2007/Aug W1
         (c) 2007 Institution of Electrical Engineers
File     6:NTIS 1964-2007/Aug W3
         (c) 2007 NTIS, Intl Cpyrght All Rights Res
File     8:Ei Compendex(R) 1884-2007/Aug W1
         (c) 2007 Elsevier Eng.  Info. Inc.
File    34:SciSearch(R) Cited Ref Sci 1990-2007/Aug W3
         (c) 2007 The Thomson Corp
File    35:Dissertation Abs Online 1861-2007/Jul
         (c) 2007 ProQuest Info&Learning
File    56:Computer and Information Systems Abstracts 1966-2007/Aug
         (c) 2007 CSA.
File    60:ANTE: Abstracts in New Tech & Engineer 1966-2007/Jul
         (c) 2007 CSA.
File    62:SPIN(R) 1975-2007/Jul W5
         (c) 2007 American Institute of Physics
```

Abstract + Npl.files
* Nothing found

```
Set     Items    Description
S1   21442996    COMPUTER?(2N)(SYSTEM? ? OR SECUR?) OR NETWORK? OR COMPUTER?
                 OR DISTRIBUT? OR ETHERNET? OR INTERNET OR INTRANET? OR LAN OR
                 LANS OR WAN OR WANS OR WLAN? ? OR VLAN? ?
S2     283082    S1(7N)((PROTECT? OR SECUR? OR GUARD? OR FORTIF? OR SHIELD?-
                 )(5N)(ACCESS? OR ENTRY OR ENTRIE? ? OR USE??? OR UTILI? OR US-
                 ING))
S3      84610    S2(7N)(ENFORC? OR CONTROL? OR REGULAT? OR DIRECT? OR MANAG?
                 OR ADMINISTRAT? OR SUSTAIN? OR ORDER??? OR MAINTAIN? OR SUPE-
                 RVIS???)
S4     307166    (ORDER?()SET? ? OR SEQUEN? OR PATTERN? OR ORDER?OR SEQUENT-
                 IAL? OR  SERIE?? OR SERIAL?? OR IN()ORDER? OR CONTIGU? OR  CO-
                 NSECUT? OR SERIAT? OR STEPWISE? OR CONSECUT? OR ONE()AFTER(2W-
                 )(OTHER OR ANOTHER))(5N)(LEVEL? OR STEP? ? OR STAGE? OR TIER??
                 ? OR OPERATION? OR FUNCTION? OR COMMAND?)
S5      23579    S4(5N)(TIME? ? OR TIMING OR TEMPORAL? OR CLOCK? OR DURATIO-
                 N? OR EVENT? OR SCHEDUL? OR OCCASION? OR DAY? ? OR HOUR? ? OR
                 MINUTE? ? OR SECOND? ? OR PERIOD?)
S6      33087    S4:S5(7N)(SECOND? OR COUPLE OR 2ND OR 2 OR DUAL?? OR TWICE
                 OR ANOTHER? OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADD-
                 ITIONAL)
S7       4917    S6(7N)(PERFORM? OR EXECUT? OR IMPLEMENT? OR OPERATE? ? OR -
                 OPERATING OR ENACT? OR HANDL? OR (CARRY? OR CARRIE? ?)()OUT OR
                 COMPLET? OR ENABL? OR ALLOW?)
S8       9378    (PRESELECT? OR PRE()SELECT? OR (SELECT? OR PICK??? OR CHOO-
                 SE? OR DESIGNAT? OR CHOSEN OR IDENT?)()BEFORE? OR PREDETERMIN?
                 OR PRE()(DETERMIN? OR SPECIF?))(5N)(ACCESS? OR ENTRY OR ENTR-
                 IE? ? OR USE??? OR UTILI?)
S9          0    S2:S3(100N)S7(100N)S8
S10         5    S2:S3(100N)S4(100N)S8
File 275:Gale Group Computer DB(TM) 1983-2007/Jul 24
         (c) 2007 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2007/Aug 13
         (c) 2007 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2007/Aug 16
         (c) 2007 The Gale Group
File  16:Gale Group PROMT(R) 1990-2007/Aug 16
         (c) 2007 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2007/Aug 14
         (c)2007 The Gale Group
File 624:McGraw-Hill Publications 1985-2007/Aug 17
         (c) 2007 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2007/Aug 17
         (c) 2007 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2007/Sep W2
         (c) 2007 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Sep W1
         (c) 2006 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2007/Aug 16
         (c) 2007 Dialog
File 369:New Scientist 1994-2007/Jul W5
         (c) 2007 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2007/Aug 17
         (c) 2007 Business Wire.
File 613:PR Newswire 1999-2007/Aug 17
```

Full Text
NPL-Files

10/3,K/5   (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire

0877285   LA039
**NOVELL LAUNCHES ITS NEXT GENERATION OPEN TRANSACTION PROCESSING MONITOR -
    TUXEDO SYSTEM 6.1**

DATE: October 31, 1995   08:36 EST   WORD COUNT: 1,163

...a fast and
efficient way to create event-based communications, enabling businesses
to trigger a **series** of processing **steps** across multiple applications in
response to **pre - specified** events;

    -- Enhanced **network**   **security**   through **Access**   **Control** Lists
(ACLs),
which provide user or group-level authorization to individual TUXEDO
services.

    TUXEDO is...